

Cisco NAC Appliance - Clean Access Manager Configuration Guide

Release 4.9(x)
March 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-28003-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Nessus is the trademark of Tenable Network Security.

Cisco NAC Appliance - Clean Access Manager includes software developed by the Apache Software Foundation (http://www.apache.org/) Copyright © 1999-2000 The Apache Software Foundation. All rights reserved. The APACHE SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS OR CISCO OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE APACHE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco NAC Appliance - Clean Access Manager Configuration Guide
© 2015 Cisco Systems, Inc. All rights reserved.



About This Guide 21

Audience 21

Purpose 21

Document Organization 22

Document Conventions 23

New Features in this Release 23

Product Documentation 24

Documentation Updates 25

Obtaining Documentation and Submitting a Service Request 26

Introduction 1-1

What is Cisco NAC Appliance? 1-1

FIPS Compliance in the Cisco NAC Appliance Network 1-2

Cisco NAC Appliance Components 1-3

Clean Access Manager (CAM) 1-5

Clean Access Server (CAS) 1-6

Cisco NAC Appliance Agents 1-7

Cisco NAC Appliance Updates 1-7

Client Login Overview 1-7

Agent Login 1-8

Web Login 1-12

Client Posture Assessment Overview 1-14

Summary Steps for Configuring Client Posture Assessment 1-14

Cisco NAC Appliance Agents 1-15

Cisco NAC Agent 1-15

Cisco NAC Web Agent 1-17

Mac OS X Agent 1-18

Clean Access Agent 1-18

Network Scanner 1-18

Managing Users 1-21

Overview of Web Admin Console Elements 1-22

Clean Access Server (CAS) Management Pages 1-23

Publishing Information 1-24

Admin Console Summary 1-25

Device Management: Adding Clean Access Servers, Adding Filters 2-1

Working with Clean Access Servers 2-2
Add Clean Access Servers to the Managed Domain 2-2
Manage the Clean Access Server 2-4
Configure Clean Access Manager-to-Clean Access Server Authorization 2-5
Summary of Steps to Configure Clean Access Manager-to-Clean Access Server Authorization 2-5
Enable Authorization and Specify Authorized Clean Access Servers 2-6
Check Clean Access Server Status 2-7
Disconnect a Clean Access Server 2-7
Reboot the Clean Access Server 2-8
Remove the Clean Access Server from the Managed Domain 2-8
Troubleshooting when Adding the Clean Access Server 2-8
Global and Local Administration Settings 2-8
Global and Local Settings 2-9
Global Device and Subnet Filtering 2-10
Overview 2-10
Device Filters and User Count License Limits 2-12
Adding Multiple Entries 2-12
Corporate Asset Authentication and Posture Assessment by MAC Address 2-12
Device Filters for In-Band Deployment 2-14
Device Filters for Out-of-Band Deployment 2-14
Device Filters for Out-of-Band Deployment Using IP Phones 2-15
In-Band and Out-of-Band Device Filter Behavior Comparison 2-16
Device Filters and Gaming Ports 2-17
Global vs. Local (CAS-Specific) Filters 2-17
Global Device Filter Lists from Cisco NAC Profiler 2-18
Configure Device Filters 2-20
Add Global Device Filter 2-20
Display/Search/Import/Export Device Filter Policies 2-23
Order Device Filter Wildcard/Range Policies 2-24
Test Device Filter Policies 2-25
View Active Layer 2 Device Filter Policies 2-26
Edit Device Filter Policies 2-27
Delete Device Filter Policies 2-27
Configure Subnet Filters 2-27
Integrating Cisco ISE Profiler 2-29
Add Cisco ISE Profiler Details 2-30

Display/Edit/Delete Cisco ISE Profiler Details 2-31
Synchronize Endpoints from Cisco ISE Profiler 2-32
Map Endpoint Policies 2-33
Create New Rule 2-33
View Rules 2-35
Edit Rules 2-35
Delete Rules 2-36
Order Rules 2-36
Configure NAC Manager in ISE Profiler 2-36
Troubleshooting when Synchronizing the Cisco ISE 2-38
Example Scenarios 2-38

Switch Management: Configuring Out-of-Band Deployment 3-1

Overview 3-1
In-Band Versus Out-of-Band 3-2
Out-of-Band Requirements 3-2
SNMP Control 3-4
Network Recovery for "Off Line" Out-of-Band Switches 3-4
Deployment Modes 3-5
Basic Connection 3-5
Out-of-Band Virtual Gateway Deployment 3-6
Flow for OOB VGW Mode 3-8
Out-of-Band Real-IP Gateway Deployment 3-10
Flow for Out-of-Band Real-IP Gateway Mode 3-12
L3 Out-of-Band Deployment 3-13
Configure Your Network for Out-of-Band 3-14
Configure Your Switches 3-15
Configuration Notes 3-15
Example Switch Configuration Steps 3-16
OOB Network Setup/Configuration Worksheet 3-21
List of MIBs and OIDs 3-22
Configure OOB Switch Management on the CAM 3-25
Add Out-of-Band Clean Access Servers and Configure Environment 3-25
Configure Global Device Filters to Ignore IP Phone MAC Addresses 3-28
Configure Group Profiles 3-28
Add Group Profile 3-29
Edit Group Profile 3-29
Configure Switch Profiles 3-30
Add Switch Profile 3-31
Configure Port Profiles 3-33

Add Port Profile 3-34
Configure VLAN Profiles 3-40
Add VLAN Profile 3-42
Edit VLAN Profile 3-43
Configure SNMP Receiver 3-45
SNMP Trap 3-45
Advanced Settings 3-46
Add and Manage Switches 3-48
Add New Switch 3-49
Search New Switches 3-50
Verify Devices 3-52
Discovered Clients 3-53
Manage Switch Ports 3-55
Ports Management Page 3-55
Manage Individual Ports (MAC Notification) 3-56
Manage Individual Ports (Linkup/Linkdown) 3-61
Assign a Port Profile to Multiple Ports Simultaneously 3-63
Config Tab 3-64
Configure Access to Authentication VLAN Change Detection 3-69
Out-of-Band Users 3-70
OOB User Sessions 3-70
Wired and Wireless User List Summary 3-71
OOB Troubleshooting 3-73
OOB Switch Trunk Ports After Upgrade 3-73
OOB Error: connected device <client_MAC> not found 3-73
Troubleshooting SNMP 3-74
Device IP Not Reachable 3-74
Fetching SysObjectID 3-74
SNMP Request Timed Out 3-74
Unknown User Name 3-75
Wrong Digest 3-75
Authorization Error 3-75
Unsupported Security Level 3-75
No Access 3-75
OOB Client MAC/IP Not Found 3-76
Message Not Within Time Window 3-76
Additional Information 3-76

Wireless LAN Controller Management: Configuring Wireless Out-of-Band Deployment 4-1

Overview 4-1

Wireless In-Band Versus Out-of-Band 4-2
Wireless Out-of-Band Requirements 4-2
DHCP Bridging Mode 4-3
SNMP Control 4-4
Summary Steps to Configure Wireless Out-of-Band 4-5
Wireless Out-of-Band Virtual Gateway Deployment 4-5
Login and Authentication Flow in Wireless OOB Virtual Gateway Mode 4-6
Configure Your Network for Wireless Out-of-Band 4-7
Configure Your Wireless LAN Controllers 4-7
Wireless LAN Controllers Configuration Notes 4-7
Example Wireless LAN Controller Configuration Steps 4-8
Create the Dynamic Interface on the Wireless LAN Controller 4-8
Create the WLAN on the Wireless LAN Controller and Enable Cisco NAC Appliance Integration 4-9
Configure SNMP on the Wireless LAN Controller 4-10
Specify the CAM as the SNMP Trap Receiver 4-11
Wireless OOB Network Setup/Configuration Worksheet 4-12
Configure Wireless LAN Controller Connection on the CAM 4-14
Add a Wireless Out-of-Band Clean Access Server and Configure Environment 4-14
Configure Group Profiles 4-15
Add Group Profile 4-15
Edit Group Profile 4-16
Configure Wireless LAN Controller Profiles 4-16
Add Wireless LAN Controller Profile 4-17
Configure SNMP Receiver 4-19
SNMP Trap 4-19
Add and Manage Wireless LAN Controllers 4-20
Add New Wireless LAN Controller 4-21
Search New Wireless LAN Controllers 4-22
Verify Devices 4-23
Discovered Wireless Clients 4-25
Config Tab 4-26
View Wireless Out-of-Band Online Users 4-27
Wireless Out-of-Band Users 4-28
Wireless OOB User Sessions 4-28
Wireless and Wired OOB User List Summary 4-28

Configuring User Login Page and Guest Access 5-1

User Login Page 5-1
Unauthenticated Role Traffic Policies 5-2

Proxy Settings 5-2
Add Default Login Page 5-3
Change Page Type (to Frame-Based or Small-Screen) 5-4
Enable Web Client for Login Page 5-5
DHCP Release/Renew with Agent/ActiveX/Java Applet 5-6
Customize Login Page Content 5-8
Create Content for the Right Frame 5-11
Upload a Resource File 5-13
Customize Login Page Styles 5-14
Configure Other Login Properties 5-15
Redirect the Login Success Page 5-15
Specify Logout Page Information 5-16
Guest User Access 5-17
Configure Guest User Registration 5-17
Configuring the Guest User Access Page 5-18
Enable the Preset "Guest" User Account 5-22

User Management: Configuring User Roles and Local Users 6-1

Overview 6-1
Create User Roles 6-2
User Role Types 6-3
Unauthenticated Role 6-3
Normal Login Role 6-4
Client Posture Assessment Roles 6-5
Session Timeouts 6-6
Default Login Page 6-7
Traffic Policies for Roles 6-7
Adding a New User Role 6-7
Role Properties 6-9
Modifying an Existing Temporary, Quarantine, or Login Role 6-14
Editing an Existing Role 6-14
Delete Role 6-15
Create Local User Accounts 6-15
Create or Edit a Local User 6-15

User Management: Configuring Authentication Servers 7-1

Overview 7-1
Adding an Authentication Provider 7-4
Kerberos 7-5

RADIUS 7-6
Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server 7-8
RADIUS Challenge-Response Impact On the Agent 7-14
Windows NT 7-15
LDAP 7-16
Configure LDAP Server with Simple Authentication 7-17
Configure LDAP Server with GSSAPI Authentication 7-18
Multiple Domain SSL 7-21
Active Directory Single Sign-On (SSO) 7-22
Windows NetBIOS SSO 7-22
Implementing Windows NetBIOS SSO 7-22
Cisco VPN SSO 7-24
Add Cisco VPN SSO Auth Server 7-25
Allow All 7-26
Guest 7-26
Configuring Authentication Cache Timeout (Optional) 7-28
Authenticating Against a Backend Active Directory 7-28
AD/LDAP Configuration Example 7-29
Map Users to Roles Using Attributes or VLAN IDs 7-31
Configure Mapping Rule 7-32
Editing Mapping Rules 7-37
Auth Test 7-39
RADIUS Accounting 7-41
Enable RADIUS Accounting 7-41
Restore Factory Default Settings 7-43
Add Data to Login, Logout or Shared Events 7-43
Add New Entry (Login Event, Logout Event, Shared Event) 7-44

User Management: Traffic Control, Bandwidth, Schedule 8-1

Overview 8-1
Global vs. Local Scope 8-3
View Global Traffic Control Policies 8-3
Add Global IP-Based Traffic Policies 8-4
Add IP-Based Policy 8-4
Edit IP-Based Policy 8-7
Add Global Host-Based Traffic Policies 8-8
Add Trusted DNS Server for a Role 8-8
Enable Default Allowed Hosts 8-9
Add Allowed Host 8-10

View IP Addresses Used by DNS Hosts 8-11
Proxy Servers and Host Policies 8-12
Add Global Layer 2 Ethernet Traffic Policies 8-12
Control Bandwidth Usage 8-13
Configure User Session and Heartbeat Timeouts 8-15
Session Timer 8-15
Heartbeat Timer 8-16
In-Band (L2) Sessions 8-16
OOB (L2) and Multihop (L3) Sessions 8-16
Session Timer / Heartbeat Timer Interaction 8-17
Configure Session Timer (per User Role) 8-17
Configure Heartbeat Timer (User Inactivity Timeout) 8-18
Configure OOB Heartbeat Timer (per User Role) 8-18
Configure Policies for Agent Temporary and Quarantine Roles 8-19
Configure Agent Temporary Role 8-19
Configure Session Timeout for the Temporary Role 8-20
Configure Traffic Control Policies for the Temporary Role 8-21
Configure Network Scanning Quarantine Role 8-22
Create Additional Quarantine Role 8-22
Configure Session Timeout for Quarantine Role 8-22
Configure Traffic Control Policies for the Quarantine Role 8-23
Example Traffic Policies 8-24
Allowing Authentication Server Traffic for Windows Domain Authentication 8-25
Allowing Traffic for Enterprise AV Updates with Local Servers 8-25
Allowing Gaming Ports 8-25
Microsoft Xbox 8-25
Other Game Ports 8-26
Adding Traffic Policies for Default Roles 8-27
Troubleshooting Host-Based Policies 8-30

Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment 9-1

Overview 9-1
Agent Configuration Steps 9-3
Add Default Login Page 9-3
Configure Agent Roles and User Profiles 9-3
Require Agent Login for Client Machines 9-3
Configure Out-of-Band Logoff 9-6
Enable Out-of-Band Logoff 9-9
Troubleshooting OOB Logoff 9-9

Configure Restricted Network Access for Agent Users 9-10
Configure Network Policy Page (Acceptable Use Policy) for Agent Users 9-11
Configure the Agent Temporary Role 9-11
Retrieving Cisco NAC Appliance Updates 9-12
View Current Updates 9-12
Configure and Download Updates 9-15
Configure Proxy Settings for CAM Updates (Optional) 9-17
Setting Up Agent Distribution/Installation 9-18
Agent Distribution 9-19
Installation Page 9-21
Cisco NAC Agent XML Configuration File Settings 9-24
Agent Customization File Settings 9-34
Logo 9-35
Agent Login Screen 9-35
Predetermined Set of Agent Strings and Fields 9-37
Cisco NAC Agent MSI Installer 9-38
Configuring Agent-Based Posture Assessment 9-40
Overview 9-40
Configuring AV/AS Definition Update Requirements 9-42
AV Rules and AS Rules 9-44
Verify AV/AS Support Info 9-45
Create an AV Rule 9-48
Create an AV Definition Update Requirement 9-51
Create an AS Rule 9-54
Create an AS Definition Update Requirement 9-56
Configuring a Windows Server Update Services Requirement 9-58
Create Windows Server Update Service Requirement 9-60
Map Windows Server Update Service Requirement to Windows Rules 9-64
Configuring a Windows Update Requirement 9-65
Create a Windows Update Requirement 9-67
Map Windows Update Requirement to Windows Rules 9-70
Configuring Custom Checks, Rules, and Requirements 9-71
Custom Requirements 9-71
Custom Rules 9-72
Cisco Pre-Configured Rules (“pr_”) 9-72
Custom Checks 9-73
Cisco Pre-Configured Checks (“pc_”) 9-73
Using Pre-Configured Rules to Check for CSA 9-73
Copying Checks and Rules 9-73

Configuration Summary 9-74
Create Custom Check 9-74
Create a Custom Rule 9-78
Validate Rules 9-80
Create a Custom Requirement 9-81
Configuring a Launch Programs Requirement 9-86
Launch Programs With Admin Privileges 9-86
Launch Programs Without Admin Privileges 9-86
Create a Launch Programs Requirement 9-89
Map Requirements to Rules 9-91
Apply Requirements to User Roles 9-93
Validate Requirements 9-94
Configuring an Optional/Audit Requirement 9-95
Configuring Auto Remediation for Requirements 9-99
Post-Configuration and Agent Maintenance on the CAM 9-101
Manually Uploading the Agent to the CAM 9-101
Downgrading the Agent 9-102
Configure Agent Auto-Upgrade 9-104
Enable Agent Auto-Upgrade on the CAM 9-104
Disable Agent Upgrades to Users 9-104
Disable Mandatory Agent Auto-Upgrade on the CAM 9-105
User Experience for Agent Auto-Upgrade 9-105
Uninstalling the Agent 9-105
Agent Auto-Upgrade Compatibility 9-107

Cisco NAC Appliance Agents 10-1

Cisco NAC Agent 10-1
Windows Cisco NAC Agent Overview 10-1
Configuration Steps for the Windows Cisco NAC Agent 10-3
Windows Cisco NAC Agent User Dialogs 10-3
RADIUS Challenge-Response Cisco NAC Agent Dialogs 10-24
Cisco NAC Web Agent 10-27
Overview 10-27
System Requirements 10-28
Configuration Steps for the Cisco NAC Web Agent 10-29
Cisco NAC Web Agent User Dialogs 10-30
Mac OS X Cisco NAC Agent 10-46
Mac OS X Cisco NAC Agent Overview 10-46
Configuration Steps for the Mac OS X Cisco NAC Agent 10-47
Mac OS X Cisco NAC Agent Configuration File Settings 10-47

Mac OS X Posture Assessment Prerequisites/Restrictions 10-47
Mac OS X Agent Prerequisites 10-47
Mac OS X Agent Restrictions 10-51
CAM/CAS Restrictions 10-51
Requirement Types Supported for Mac OS X Agent 10-51
Mac OS X Cisco NAC Agent Dialogs 10-52
Mac OS X Cisco NAC Agent Application File Locations 10-67
RADIUS Challenge-Response Mac OS X Cisco NAC Agent Dialogs 10-69

Monitoring and Troubleshooting Agent Sessions 11-1
Viewing Agent Reports 11-1
Exporting Agent Reports 11-5
Limiting the Number of Reports 11-6
Create Agent Log Files Using the Cisco Log Packager 11-6
Manage Certified Devices 11-10
Add Exempt Device 11-12
Clear Certified or Exempt Devices Manually 11-13
View Reports for Certified Devices 11-13
View Switch/WLC Information for Out-of-Band Certified Devices 11-13
Configure Certified Device Timer 11-14
Add Floating Devices 11-16
Report Settings 11-18
Dashboard 11-18
Current Status 11-18
CCA Servers 11-20
Managed Switches 11-20
Authentication Servers 11-21
User Statistics 11-22
Custom **Reports** 11-22
Generate New Reports 11-22
View Saved Templates 11-26
View Executive Summary 11-26
Configuration 11-27
User Activity Log Files 11-27
Online Users list 11-28
Interpreting Active Users 11-29
View Online Users 11-30
In-Band Users 11-31
Out-of-Band Users 11-31
Display Settings 11-35

Agent Troubleshooting 11-36
Debug Logging for Cisco NAC Appliance Agents 11-37
Generate Cisco NAC Agent Debug Logs 11-37
Cisco NAC Web Agent Logs 11-37
Generate Mac OS X Agent Debug Log 11-37
Client Cannot Connect/Login 11-38
No Agent Pop-Up/Login Disabled 11-38
Client Cannot Connect (Traffic Policy Related) 11-39
AV/AS Rule Troubleshooting 11-40
Cisco NAC Web Agent Status Codes 11-40
Known Issue for Windows Script 5.6 11-41
Known Issue for MS Update Scanning Tool (KB873333) 11-41

Configuring Network Scanning 12-1
Overview 12-1
Network Scanning Implementation Steps 12-3
User Page Summary 12-4
Configure the Quarantine Role 12-6
Load Nessus Plugins into the Clean Access Manager Repository 12-6
Uploading Plugins 12-7
Deleting Plugins 12-8
Configure General Setup 12-9
Apply Plugins 12-10
Configure Plugin Options 12-12
Configure Vulnerability Handling 12-13
Test Scanning 12-16
Show Log 12-17
View Scan Reports 12-17
Customize the User Agreement Page 12-19

Monitoring Event Logs 13-1
Overview 13-1
Interpreting Event Logs 13-4
View Logs 13-4
Event Log Example 13-8
Limiting the Number of Logged Events 13-9
Configuring Syslog Logging 13-9
Cisco NAC Appliance Log Files 13-11
Log File Sizes 13-11

SNMP 13-13
Enable SNMP Polling/Alerts 13-14
Add New Trapsink 13-15
SNMP on Individual CAS 13-18
Add New Trapsink to CAS 13-19

Administering the CAM 14-1
Overview 14-1
Network 14-2
Failover 14-4
Set System Time 14-5
Manage CAM SSL Certificates 14-7
SSL Certificate Overview 14-7
Web Console Pages for SSL Certificate Management 14-8
Typical SSL Certificate Setup on the CAM 14-9
Phase 1: Prepare Your CAM and CAS for the Certificate Signing Request (CSR) 14-9
Phase 2: Prepare your CAM and CAS For CA-Signed Certs (Production Deployment) 14-9
Phase 3: Adding a New CAM or CAS to an Existing Production Deployment 14-10
Generate Temporary Certificate 14-11
Generate and Export a Certification Request (Non-FIPS CAM Only) 14-12
Manage Signed Certificate/Private Key 14-14
Import Signed Certificate/Private Key 14-14
Export Certificate and/or Private Key 14-16
Manage Trusted Certificate Authorities 14-16
Import/Export Trusted Certificate Authorities 14-18
View Current Private Key/Certificate and Certificate Authority Information 14-19
Troubleshooting Certificate Issues 14-21
HA Active-Active Situation Due to Expired SSL Certificates 14-21
No Web Login Redirect/CAS Cannot Establish Secure Connection to CAM 14-22
Private Key in Clean Access Server Does Not Match the CA-Signed Certificate 14-23
Regenerating Certificates for DNS Name Instead of IP 14-23
Disabling Administrator Prompt for Certificate on IE 8 and 9 14-23
Certificate-Related Files 14-24
System Upgrade 14-24
Licensing 14-25
Policy Import/Export 14-28
Policy Sync Policies 14-28
Policies Excluded from Policy Sync 14-29
Example Scenarios 14-29

Policy Sync Configuration Summary 14-30
Before You Start 14-30
Enable Policy Sync on the Master 14-31
Configure the Master 14-32
Enable Policy Sync on the Receiver 14-34
Configure the Receiver 14-35
Perform Policy Sync 14-36
Perform Manual Sync 14-37
Perform Auto Sync 14-38
Verify Policy Sync 14-39
View History Logs 14-39
Troubleshooting Manual Sync Errors 14-41
Support Logs 14-42
Filtering Logs by CAS and/or Agent IP 14-45
Agent Logs 14-46
Admin Users 14-47
Admin Groups 14-47
Add/Edit a Custom Admin Group 14-47
Admin Users 14-50
Login/Logout an Admin User 14-51
Add an Admin User 14-51
Edit an Admin User 14-52
Active Admin User Sessions 14-53
Administrator User Access Restrictions 14-54
Manage System Passwords 14-56
Change the CAM Web Console Admin Password 14-57
Change the CAS Web Console Admin User Password 14-57
Backing Up the CAM Database 14-58
Automated Daily Database Backups 14-59
Manual Backups from Web Console 14-59
Restoring a CAM Snapshot—Standalone CAM 14-60
Restoring a CAM Snapshot—HA-CAM or HA-CAS 14-61
Backing Up and Restoring CAM/CAS Authorization Settings 14-62
Database Recovery Tool 14-64
API Support 14-65

Error and Event Log Messages A-1

Client Error Messages A-1
Login Failed A-1

Network Error A-1
Users Cannot Log In During CAS Fallback Recovery A-2
CAM Event Log Messages A-2

API Support B-1
Overview B-1
Authentication Requirements B-2
Administrator Operations B-2
adminlogin B-2
<any subsequent operation> B-2
adminlogout B-3
Device Filter Operations B-3
addmac B-3
removemac B-4
checkmac B-4
getmaclist B-5
removemaclist B-5
addsubnet B-6
updatesubnet B-6
removesubnet B-6
Synchronizing with ISE Profiler Operations B-7
profilerEndpointEvent B-7
resyncwithprofiler B-7
Certified Devices List Operations B-7
addcleanmac B-8
removecleanmac B-8
clearcertified B-9
User Operations B-9
kickuser B-9
kickuserbymac B-10
kickoobuser B-10
queryuserstime B-10
renewuserstime B-11
changeuserrole B-11
changeloggedinuserrole B-11
Guest Access Operations B-12
getlocaluserlist B-12
addlocaluser B-13
deletelocaluser B-13

OOB Switch Management Operations B-13
bounceport B-14
bounceportbymac B-14
Report Operations B-14
getversion B-15
getuserinfo B-15
getoobuserinfo B-16
getcleanuserinfo B-16
getreports B-16
getuallist B-21
getualfile B-21
getcannedreportslist B-22
getcannedreport B-22

MIB Support C-1

Open Source License Acknowledgements D-1
Notices D-1
OpenSSL/Open SSL Project D-1
License Issues D-1

INDEX



About This Guide

Revised March 10, 2015, OL-28003-01

This preface includes the following sections:

- Audience
- Purpose
- Document Organization
- Document Conventions
- New Features in this Release
- Product Documentation
- Documentation Updates
- Obtaining Documentation and Submitting a Service Request

Audience

This guide is for network administrators who are implementing the Cisco NAC Appliance solution to manage and secure their networks. Cisco NAC Appliance comprises the Clean Access Manager (CAM) administration appliance, Clean Access Server (CAS) enforcement appliance, and Agent end-user client software. Use this document along with the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)* and *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* to install, configure, and administer your Cisco NAC Appliance deployment.

Purpose

The *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)* describes how to configure the Clean Access Manager NAC Appliance for Cisco NAC Appliance, Releases 4.9(2), 4.9(3), 4.9(4), and 4.9(5). You can use the Clean Access Manager (CAM) and its web-based administration console to manage multiple Clean Access Servers (CASs) in a deployment. End users connect through the Clean Access Server to the network via web login or Agent. This guide describes how to use the CAM web administration console to configure most aspects of Cisco NAC Appliance. It also provides information specific to the Clean Access Manager, such as how to manage network switches in an Out-of-Band deployment. See Product Documentation for further details on the document set for Cisco NAC Appliance.

Document Organization

Table 1 Document Organization

Chapter	Description
Chapter 1, "Introduction"	Provides a high-level overview of the Cisco NAC Appliance solution
Chapter 2, "Device Management: Adding Clean Access Servers, Adding Filters"	Describes how to add and manage Clean Access Servers from the Clean Access Manager and configure device and/or subnet filters
Chapter 3, "Switch Management: Configuring Out-of-Band Deployment"	Describes how to configure Cisco NAC Appliance for Out-of-Band (OOB) deployment
Chapter 4, "Wireless LAN Controller Management: Configuring Wireless Out-of-Band Deployment"	Describes how to configure Cisco NAC Appliance for Wireless Out-of-Band (Wireless OOB) deployment.
Chapter 5, "Configuring User Login Page and Guest Access"	Explains how to add the default login page needed for all users to authenticate, customize the login page for web login users, and configure Cisco NAC Appliance for guest user login
Chapter 6, "User Management: Configuring User Roles and Local Users"	Explains how to create user roles and new user profiles
Chapter 7, "User Management: Configuring Authentication Servers"	Describes how to set up external authentication sources, configure Active Directory Single Sign-On (SSO), VLAN ID or attribute-based auth server mapping rules, and RADIUS accounting
Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule"	Describes how to configure role-based traffic control policies, bandwidth management, session and heartbeat timers
Chapter 9, "Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment"	Describes how to configure Agent distribution and installation for client machines, as well as configure client posture assessment in the Cisco NAC Appliance system
Chapter 10, "Cisco NAC Appliance Agents"	Presents overviews, login flow, and session termination dialogs for the Cisco NAC Appliance Agents (Cisco NAC Agent and Cisco NAC Web Agent)
Chapter 11, "Monitoring and Troubleshooting Agent Sessions"	Provides information on compiling and accessing various Cisco NAC Appliance Agent reports and log files and troubleshooting Agent connection and operation issues
Chapter 12, "Configuring Network Scanning"	Describes how to set up network scanning for Cisco NAC Appliance
Chapter 13, "Monitoring Event Logs"	Describes the Monitoring module of Cisco NAC Appliance, including online users, event logs, and SNMP information

Table 1 Document Organization

Chapter	Description
Chapter 14, "Administering the CAM"	Discusses the Administration pages for the Clean Access Manager
Appendix A, "Error and Event Log Messages"	Explains some common Cisco NAC Appliance error messages and event log entries
Appendix B, "API Support"	Discusses API support for the Clean Access Manager
Appendix C, "MIB Support"	Contains the list of Entities and Object Identifiers (OIDs) for the MIBs supported by CAM
Appendix D, "Open Source License Acknowledgments"	Contains Open Source License information for Cisco products

Document Conventions

Table 2 Document Conventions

Item	Convention
Indicates command line output.	`Screen` font
Indicates information you enter.	**`Boldface screen`** font
Indicates variables for which you supply values.	*`Italic screen`* font
Indicates web admin console modules, menus, tabs, links and submenu links.	**Boldface** font
Indicates a menu item to be selected.	**Administration > User Pages**

New Features in this Release

For a brief summary of the new features and enhancements available in this release refer to Documentation Updates and the "New and Changed Information" section of the *Release Notes for Cisco NAC Appliance* corresponding to your latest Cisco NAC Appliance release version.

Product Documentation

Table 3 lists documents are available for Cisco NAC Appliance on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html

Tip To access external URLs referenced in this document, right-click the link in Adobe Acrobat and select "Open in Weblink in Browser."

Table 3 Cisco NAC Appliance Document Set

Document Title	Refer to This Document For Information On:
Cisco NAC Appliance Service Contract/Licensing Support	• Obtaining and installing product licenses • Information on service contracts, ordering and RMA
Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later	• Agent System Requirements, Agent/Server Version Compatibility, Agent/OS/Browser Support Matrix, Agent/AD Server Compatibility for AD SSO, and Agent Localized Language Template Support
Cisco NAC Appliance Switch and Wireless LAN Controller Support	• Which switches and NMEs support OOB deployment • Known issues/troubleshooting for switches and WLCs
Getting Started with Cisco NAC Network Modules in Cisco Access Routers	• Installing or upgrading the Clean Access Server (CAS) software on the Cisco NAC network module (NME-NAC-K9)
Connecting Cisco Network Admission Control Network Modules	• Connecting Cisco NAC network module (NME-NAC-K9) in an Integrated Services Router
Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide	• Provides instructions to upgrade your existing Cisco NAC-3310, NAC-3350, and NAC-3390 with a field-replaceable FIPS card necessary to introduce FIPS compliance in your network
Release Notes for Cisco NAC Appliance	Details on the latest 4.9(x) release, including: • New features and enhancements • Fixed caveats • Upgrade instructions • Supported AV/AS product charts • CAM/CAS/Agent compatibility and version information

Table 3 Cisco NAC Appliance Document Set

Document Title	Refer to This Document For Information On:
Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)	Details on CAM/CAS installation topics: • Hardware specifications on the various CAM/CAS platforms • How to install the Clean Access Manager and Clean Access Server Platforms • How to install Cisco NAC Appliance software on the CASM/CAS • How to configure CAM and CAS pairs for High Availability
Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)	Complete CAM details, including: • How to install the CAM software • Overviews of major concepts and features of Cisco NAC Appliance • How to use the CAM web console to perform global configuration of Cisco NAC Appliance (applying to all CASs in the deployment) • How to configure CAM pairs for High Availability
Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)	CAS-specific details, including: • How to install the CAS software • Where to deploy the CAS on the network (general information) • How to perform local (CAS-specific) configuration using the CAS management pages of the CAM web console, or the CAS direct access console. • How to configure CAS pairs for High Availability

Documentation Updates

Table 4 Updates to Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)

Date	Description
03/09/2015	Release 4.9(5) • Updated System Upgrade, page 24 • Updated Release 4.9(5) screenshots as appropriate

Table 4 Updates to Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x) (continued)

Date	Description
02/10/2014	Release 4.9(4) • Updated System Upgrade, page 24 • Updated Release 4.9(4) screenshots as appropriate
06/25/2013	Release 4.9(3) • Updated System Upgrade, page 24 • Updated Release 4.9(3) screenshots as appropriate
11/27/2012	Release 4.9(2)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



Introduction

This chapter provides a high-level overview of the Cisco NAC Appliance solution. Topics include:

- What is Cisco NAC Appliance?, page 1-1
- FIPS Compliance in the Cisco NAC Appliance Network, page 1-2
- Cisco NAC Appliance Components, page 1-3
- Client Posture Assessment Overview, page 1-13
- Client Login Overview, page 1-6
- Managing Users, page 1-20
- Overview of Web Admin Console Elements, page 1-21
- Clean Access Server (CAS) Management Pages, page 1-22
- Admin Console Summary, page 1-24

What is Cisco NAC Appliance?

The Cisco Network Admission Control (NAC) Appliance (formerly known as Cisco Clean Access) is a powerful, easy-to-use admission control and compliance enforcement solution. With comprehensive security features, In-Band or Out-of-Band deployment options, user authentication tools, and bandwidth and traffic filtering controls, Cisco NAC Appliance is a complete solution for controlling and securing networks. As the central access management point for your network, Cisco NAC Appliance lets you implement security, access, and compliance policies in one place instead of having to propagate the policies throughout the network on many devices.

The security features in Cisco NAC Appliance include user authentication, policy-based traffic filtering, and client posture assessment and remediation. Cisco NAC Appliance stops viruses and worms at the edge of the network. With remote or local system checking, Cisco NAC Appliance lets you block user devices from accessing your network unless they meet the requirements you establish.

Cisco NAC Appliance is a network-centric integrated solution administered from the web console of the Clean Access Manager (CAM) administration server and enforced through the Clean Access Server (CAS) and the Cisco NAC Agent/Cisco NAC Web Agent. You can deploy the Cisco NAC Appliance in the configuration that best meets the needs of your network. The Clean Access Server can be deployed as the first-hop gateway for your edge devices providing simple routing functionality, advanced DHCP services, and other services. Alternatively, if elements in your network already provide these services, the CAS can work alongside those elements without requiring changes to your existing network by being deployed as a “bump-in-the-wire.”

Other key features of Cisco NAC Appliance include:

- Standards-based architecture—Uses HTTP, HTTPS, XML, and Java Management Extensions (JMX).
- User authentication—Integrates with existing backend authentication servers, including Kerberos, LDAP, RADIUS, and Windows NT domain.
- VPN concentrator integration—Integrates with Cisco VPN concentrators (e.g. VPN 3000, ASA) and provides Single Sign-On (SSO).
- Active Directory SSO—Integrates with Active Directory on Windows Servers to provide Single Sign-On for Cisco NAC Agent users logging into Windows systems. (Cisco NAC Web Agent does not support SSO.)
- Cisco NAC Appliance compliance policies—Allows you to configure client posture assessment and remediation via use of Agent.

  The Cisco NAC Web Agent performs posture assessment, but does not provide a medium for remediation. The user must manually fix/update the client machine and "Re-Scan" to fulfill posture assessment requirements with the Web Agent.

  The Cisco NAC Agent does not support Nessus-based network scanning.
- Layer 2 or Layer 3 deployment options—The Clean Access Server can be deployed within L2 proximity of users, or multiple hops away from users. You can use a single CAS for both L3 and L2 users.
- In-Band (IB) or Out-of-Band (OOB) deployment options—Cisco NAC Appliance can be deployed in-line with user traffic, or Out-of-Band to allow clients to traverse the network only during posture assessment and remediation while bypassing it after certification (posture assessment).
- Traffic filtering policies—Role-based IP and host-based policies provide fine-grained and flexible control for In-Band network traffic.
- Bandwidth management controls—Limit bandwidth for downloads or uploads.
- High availability—Active/Passive failover (requiring two servers) ensures services continue if an unexpected shutdown occurs. You can configure pairs of Clean Access Manager (CAM) machines and/or CAS machines in high-availability mode.



Note Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

FIPS Compliance in the Cisco NAC Appliance Network

Cisco NAC Appliance Release 4.7(0), 4.8, and 4.9 support Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance for new installations on new Cisco NAC-3315, NAC-3355, and NAC-3395 hardware appliance platforms and Cisco NAC-3310, NAC-3350, and NAC-3390 platforms in which you have installed a field-replaceable FIPS card as described in the *Cisco NAC Appliance FIPS Field-Replaceable Unit Installation Guide*. In order to provide FIPS compliance in your Cisco NAC Appliance network, both CAM(s) and CAS(s) must use the new hardware platforms and be FIPS compliant.

To enable FIPS 140-2 compliance in Cisco NAC Appliance, the CAMs/CASs must have an encryption card installed that handles the primary FIPS "level 2" compliance functions and manages private keys for the system. To also enhance network security and adhere to FIPS 140-2 compliance, Cisco NAC

Appliance encapsulates SWISS communications between client machines and CASs, including Discovery packet transmission/acknowledgement, authentication, and posture assessment results using the HTTPS protocol. The SWISS mechanism also features an enhanced handler that uses 3DES encryption for SWISS protocol functions.

In addition, there are several specific tasks you must perform to ensure your Cisco NAC Appliance network remains FIPS compliant:

- Obtain appropriate next generation FIPS-compliant hardware as described in the "Cisco NAC Appliance Hardware Platforms" chapter of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*
- Install and appropriately configure the same next generation FIPS-compliant hardware as described in the "Installing the Clean Access Manager and Clean Access Server" chapter of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*
- If necessary, enable the TLSv1 option in Internet Explorer version 6 by following the guidelines in the "Enabling TLSv1 on Internet Explorer Version 6" installation troubleshooting section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*
- Ensure your CAM/CAS SSL certificates adhere to the guidelines outlined in Manage CAM SSL Certificates, page 14-7 and the "Manage CAS SSL Certificates" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*
- Specify the appropriate encryption protocols for Out-of-Band switch management according to the guidelines in Configure SNMP Receiver, page 3-44
- Configure connections to external RADIUS authentication servers according to the guidelines in RADIUS, page 7-6 and Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server, page 7-8
- Configure Cisco NAC Appliance to perform VPN SSO via a Cisco ASA in a FIPS-compliant network according to the guidelines in the "Adding/Editing VPN Concentrator Entries," "Adding/Editing Accounting Server Entries," and "Configure VPN SSO in a FIPS 140-2 Compliant Deployment" sections of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*
- Configure Cisco NAC Appliance to perform AD SSO for Windows Client machines in a FIPS 140-2 compliant network according to the guidelines in "Configure Active Directory for FIPS 140-2 Compliant AD SSO" section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x).*
- Ensure you disable Network Time Protocol (NTP) server authentication on both the CAM and CAS using the instructions at Set System Time, page 14-5 and the "Synchronize System Time" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*

Note Cisco NAC Appliance Release 4.7(0), 4.8, and 4.9 are the only tested FIPS 140-2 compliant releases.

Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.7(0), 4.8, and 4.9.

Cisco NAC Appliance Components

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager web console and enforced through the Clean Access Server and (optionally) the Agent. Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation **before** clients access the network. Cisco NAC Appliance consists of the following components (in Figure 1-1):

- **Clean Access Manager (CAM)**—Administration server for Cisco NAC Appliance deployment. The secure web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment (or 40 CASs if installing a SuperCAM). For Out-of-Band (OOB) deployment, the web admin console allows you to control switches and VLAN assignment of user ports through the use of SNMP.

  Note The CAM web admin console supports Internet Explorer 6.0 or above only, and requires high encryption (64-bit or 128-bit). High encryption is also required for client browsers for web login and Agent authentication.

- **Clean Access Server (CAS)**—Enforcement server between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Cisco NAC Appliance system requirements.

  You can install a CAS as either a stand-alone appliance (like the Cisco NAC-3300 series) or as a network module (Cisco NME-NAC-K9) in a Cisco ISR chassis and deploy it In-Band (always inline with user traffic) or Out-of-Band (inline with user traffic only during authentication/posture assessment). The CAS can also be deployed in Layer 2 mode (users are L2-adjacent to CAS) or Layer 3 mode (users are multiple L3 hops away from the CAS).

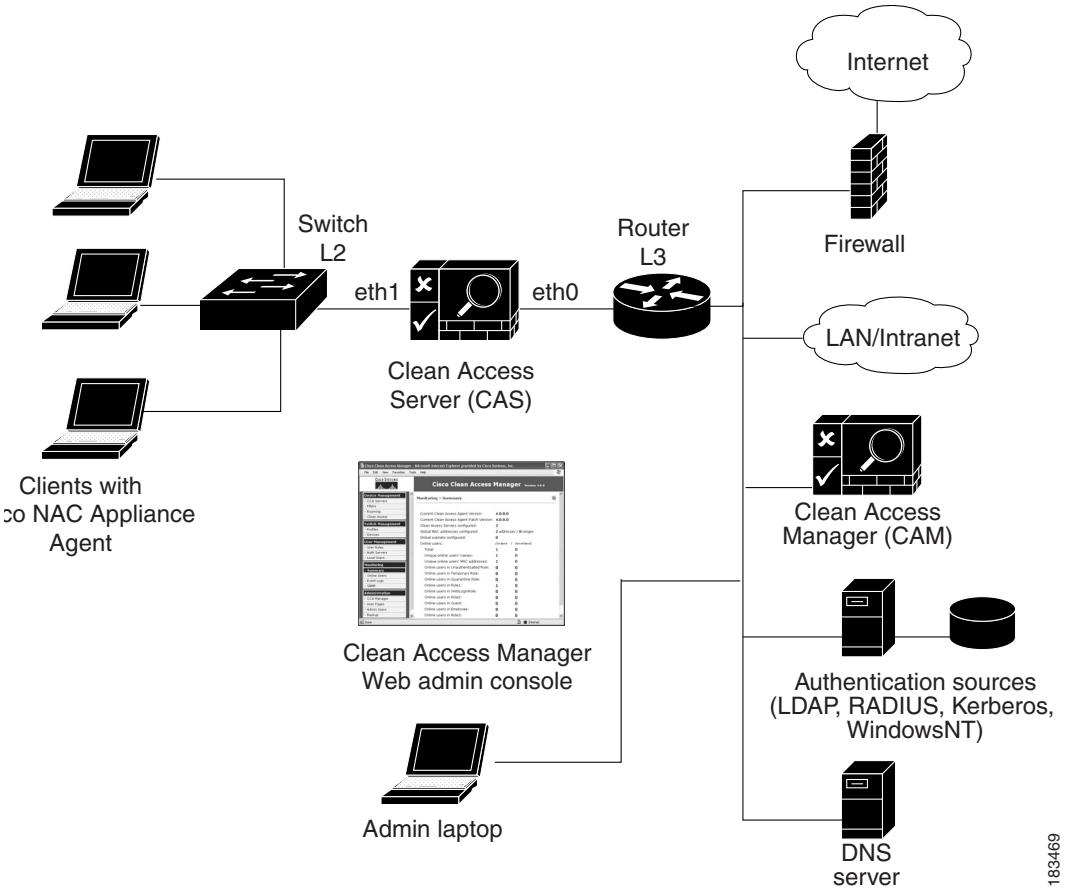
  You can also deploy several CASs of varying size/capacity to fit the needs of varying network segments. You can install Cisco NAC-3300 series appliances in your company headquarters core, for example to handle thousands of users and simultaneously install one or more Cisco NAC network modules in ISR platforms to accommodate smaller groups of users at a satellite office, for example.

- **Cisco NAC Appliance Agents**—Optional read-only persistent or temporal Agents that reside on client machines. Cisco NAC Appliance Agent check applications, files, services, or registry keys to ensure that client machines meet your specified network and software requirements prior to gaining access to the network.

  Note There is no client firewall restriction with client posture assessment via the Agent. The Agent can check the client registry, services, and applications even if a personal firewall is installed and running.

- **Cisco NAC Appliance Updates**—Regular updates of pre-packaged policies/rules that can be used to check the up-to-date status of operating systems, antivirus (AV), antispyware (AS), and other client software. Provides built-in support for AV vendors and AS vendors.

Figure 1-1 Cisco NAC Appliance Deployment (L2 In-Band Example)



Clean Access Manager (CAM)

The Clean Access Manager (CAM) is the administration server and database which centralizes configuration and monitoring of all Clean Access Servers, users, and policies in a Cisco NAC Appliance deployment. You can use it to manage up to 20 Clean Access Servers. The web admin console for the Clean Access Manager is a secure, browser-based management interface. See Admin Console Summary, page 1-24 for a brief introduction to the modules of the web console. For Out-of-Band (OOB) deployment, the web admin console provides the **OOB Management** module to add and control switches in the Clean Access Manager's domain and configure switch ports.

Clean Access Server (CAS)

The Clean Access Server (CAS) is the gateway between an untrusted and trusted network. The Clean Access Server can operate in one of the following In-Band (IB) or Out-of-Band (OOB) modes:

- IB Virtual Gateway (L2 transparent bridge mode)
- IB Real-IP Gateway
- OOB Virtual Gateway
- OOB Real-IP Gateway

This guide describes the global configuration and administration of Clean Access Servers and Cisco NAC Appliance deployment using the Clean Access Manager web admin console.

For a summary of CAS operating modes, see Add Clean Access Servers to the Managed Domain, page 2-2. For complete details on CAS deployment, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

For details on OOB implementation and configuration, see Chapter 3, "Switch Management: Configuring Out-of-Band Deployment."

For details on options configured locally on the CAS, such as DHCP configuration, Cisco VPN Concentrator integration, or local traffic policies, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Cisco NAC Appliance Agents

When enabled for your Cisco NAC Appliance deployment, the Agent can ensure that computers accessing your network meet the system requirements you specify. The Agent is a read-only, easy-to-use, small-footprint program that resides on Windows user machines. When a user attempts to access the network, the Agent checks the client system for the software you require, and helps users acquire any missing updates or software.

Agent users who fail the system checks you have configured are assigned to the Agent Temporary role. This role gives users limited network access to access the resources needed to comply with the Agent requirements. Once a client system meets the requirements, it is considered "clean" and allowed network access.

The Cisco NAC Appliance Agent types available in Cisco NAC Appliance are:

- Cisco NAC Agent (persistent Agent for Windows client machines)
- Windows Clean Access Agent (persistent Agent for Windows client machines available prior to release 4.6(1))
- Mac OS X Agent (persistent Agent for Macintosh client machines)
- Cisco NAC Web Agent (temporal Agent for Windows client machines)

For more information on the Agent types available in Cisco NAC Appliance, see Chapter 10, "Cisco NAC Appliance Agents."

Cisco NAC Appliance Updates

Regular updates of pre-packaged policies/rules can be used to check the up-to-date status of operating systems, antivirus/antispyware software, and other client software. Cisco NAC Appliance provides built-in support for major AV and AS vendors. For complete details, see Retrieving Cisco NAC Appliance Updates, page 9-12.

Client Login Overview

Agent scanning and/or network scanning must first be enabled under **Device Management > Clean Access > General Setup** before configuring posture assessment.

- The Agent Login subpage enables Agent controls per user role/OS.

- The Web Login subpage enables network scanning controls per user role/OS.

In addition to dialog/web page content, you can specify whether pages appear when the user logs in with a specific user role and OS. If you want to enable both Agent and network scanning for a role, make sure to set role/OS options on both the **Agent Login** and **Web Login** configuration pages.

Note Agent/network scanning pages are always configured by both user role and client OS.

Agent Login

Agent users see the web login page and the Agent download page the first time they perform initial web login in order to download and install the Agent setup installation file. After installation, Agent users should login through the Agent dialog which automatically pops up when "**Popup Login Window**" is selected from the system tray icon menu (default setting). Cisco NAC Agent users can also bring up the login dialog by right-clicking the Agent system tray icon and selecting "**Login**." Cisco NAC Web Agent users are automatically connected to the network once their client machine is scanned and found compliant with Agent Requirement settings.

Note Agent Login/Logout is disabled (grayed out) for special logins, such as VPN SSO, AD SSO, and MAC address-based login. The Logout option is not needed for these deployments, since the machine always attempts to log back in immediately.

Agent users will not see Quarantine role pages or popup scan vulnerability reports, as the Agent dialogs perform the communication. You can also configure a Network Policy page (Acceptable Use Page) that Agent users must accept after login and before accessing the network.

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the end-user Agent login session may feature extra authentication challenge-response dialogs not available in other dialog sessions—beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager or Clean Access Server. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session.

Note Ensure that your RADIUS server and associated clients are configured to interact correctly according to the RADIUS authentication method you choose.

Figure 1-2 Agent Login—General Setup

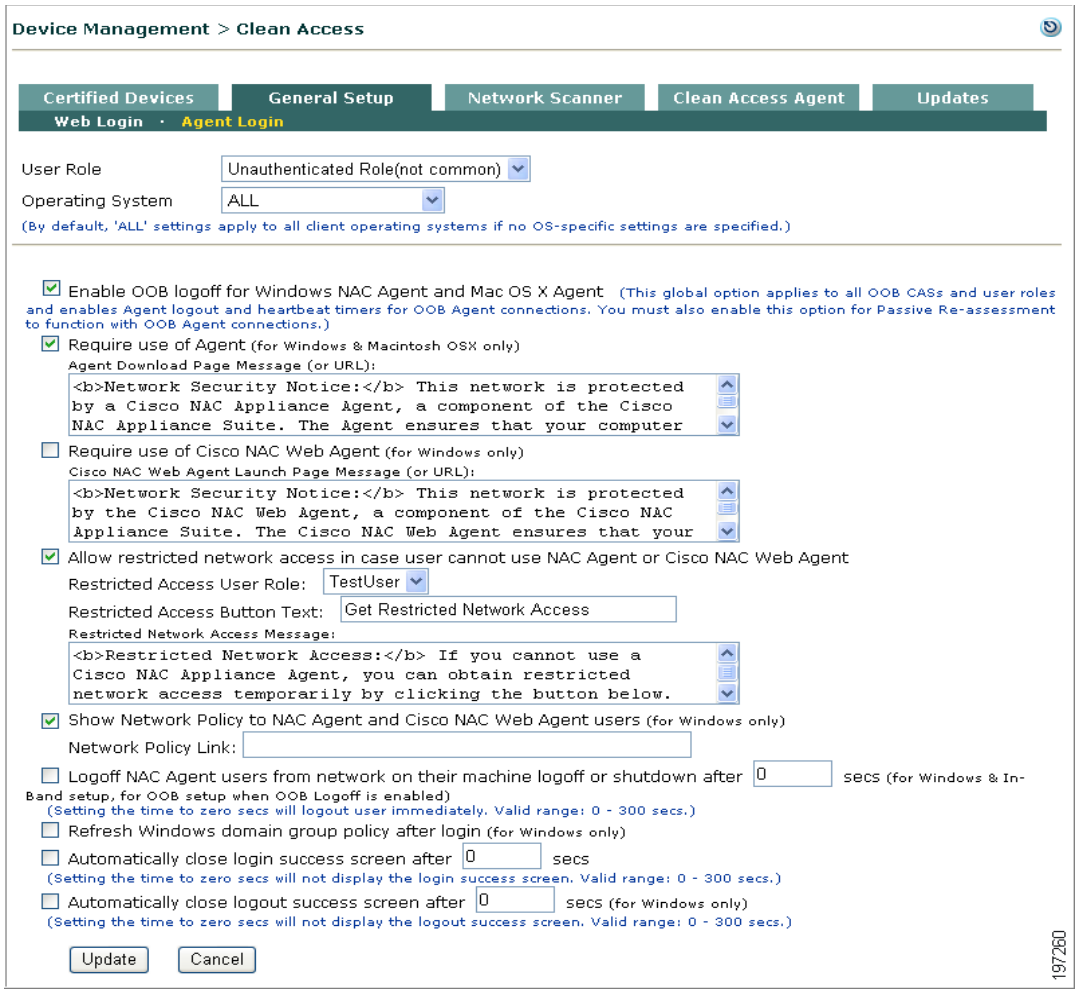

Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Web Login · Agent Login
User Role
Unauthenticated Role(not common)
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
Enable OOB logoff for Windows NAC Agent and Mac OS X Agent (This global option applies to all OOB CASs and user roles and enables Agent logout and heartbeat timers for OOB Agent connections. You must also enable this option for Passive Re-assessment to function with OOB Agent connections.)
Require use of Agent (for Windows & Macintosh OSX only)
Agent Download Page Message (or URL):
Network Security Notice: This network is protected by a Cisco NAC Appliance Agent, a component of the Cisco NAC Appliance Suite. The Agent ensures that your computer
Require use of Cisco NAC Web Agent (for Windows only)
Cisco NAC Web Agent Launch Page Message (or URL):
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco NAC Appliance Suite. The Cisco NAC Web Agent ensures that your
Allow restricted network access in case user cannot use NAC Agent or Cisco NAC Web Agent
Restricted Access User Role: TestUser
Restricted Access Button Text: Get Restricted Network Access
Restricted Network Access Message:
Restricted Network Access: If you cannot use a Cisco NAC Appliance Agent, you can obtain restricted network access temporarily by clicking the button below.
Show Network Policy to NAC Agent and Cisco NAC Web Agent users (for Windows only)
Network Policy Link:
Logoff NAC Agent users from network on their machine logoff or shutdown after 0 secs (for Windows & In-Band setup, for OOB setup when OOB Logoff is enabled)
(Setting the time to zero secs will logout user immediately. Valid range: 0 - 300 secs.)
Refresh Windows domain group policy after login (for Windows only)
Automatically close login success screen after 0 secs
(Setting the time to zero secs will not display the login success screen. Valid range: 0 - 300 secs.)
Automatically close logout success screen after 0 secs (for Windows only)
(Setting the time to zero secs will not display the logout success screen. Valid range: 0 - 300 secs.)
Update
Cancel
197260

Table 1-1 explains the **General Setup > Agent Login** configuration options shown in Figure 1-2. For examples and descriptions of Agent login user pages, see Chapter 10, "Cisco NAC Appliance Agents."

Table 1-1 Agent Login—General Setup Configuration Options

Control	Description
User Role	Choose a user role from the dropdown menu, which shows all roles in the system. Configure Agent Login settings for each role for which the Agent will be required. (See Adding a New User Role, page 6-7 for how to create new user roles.)
Operating System	Choose the client OS for the specified user role. **ALL** settings apply by default to all client operating systems if no OS-specific settings are specified. **WINDOWS_ALL** apply to all Windows operating systems if no Windows-OS specific settings are specified.

Table 1-1 Agent Login—General Setup Configuration Options (continued)

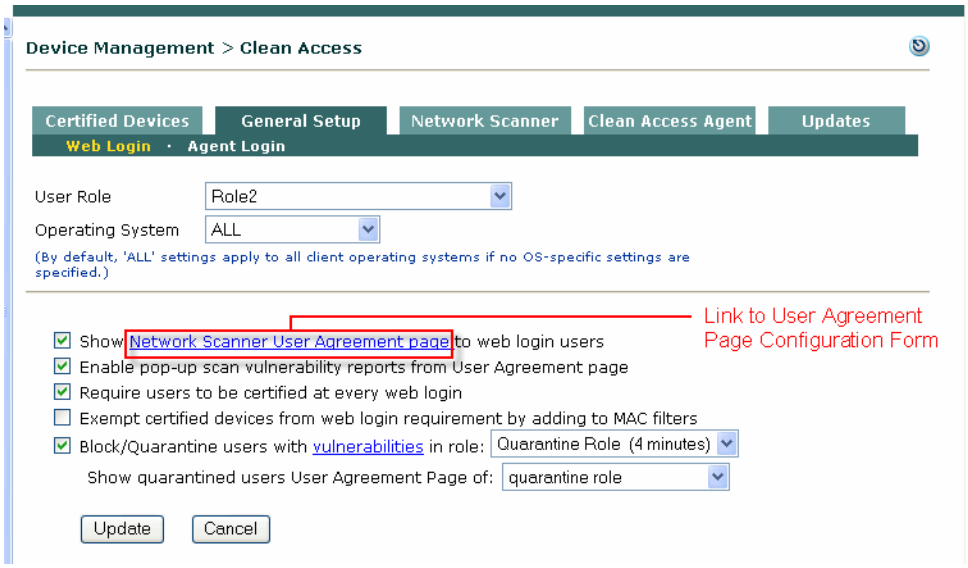
Control	Description
Enable OOB logoff for Windows NAC Agent and Mac OS X Agent	Check this option to enable OOB Logoff. This option applies globally to all OOB CASs and user roles and enables Agent logout and heartbeat timers for OOB Agent connections. You must also enable this option for Passive Re-assessment to function with OOB Agent connections. See Configure Out-of-Band Logoff, page 9-6 for more details.
Require use of Agent (for Windows and Macintosh OSX only)	Click this checkbox to redirect clients in the selected user role and OS to the **Agent Download Page Message** (or URL) after the initial web login. Users will be prompted to download, install, and use the Agent to log into the network. To modify the default download instructions, type HTML text or enter a URL. **Note** Agent requirement configuration must also be completed as described in Configuring Agent-Based Posture Assessment, page 9-39 The **Require use of Agent** and **Require use of Cisco NAC Web Agent** options are *not* mutually exclusive. If you choose to enable both options, both choices appear to users when they are directed to the Login Page.
Require use of Cisco NAC Web Agent (for Windows only)	Click this checkbox to redirect clients in the selected user role and OS to the **Cisco NAC Web Agent Download Page Message** (or URL) after the initial web login. Users will be prompted to download, install, and access the network using the temporal Cisco NAC Web Agent. To modify the default download instructions, type HTML text or enter a URL. **Note** Agent requirement configuration must also be completed as described in Configuring Agent-Based Posture Assessment, page 9-39 The **Require use of Agent** and **Require use of Cisco NAC Web Agent** options are *not* mutually exclusive. If you choose to enable both options, both choices appear to users when they are directed to the Login Page.
Allow restricted network access in case user cannot use NAC Agent and Cisco NAC Web Agent	Click this optional checkbox to allow users to have restricted network access if they choose not to install the Cisco NAC Agent or launch the Cisco NAC Web Agent. This feature is intended primarily to allow access for users logging into a user role that requires an Agent, but who have systems on which they cannot download and install the Agent (as in the case of inadequate/non-admin privileges on the machine, for example). Users can also take advantage of "restricted" network access to gain limited network access when the client machine fails remediation and the user must implement updates to meet network access requirements before they can log in using their assigned user role. For details, see Configure Restricted Network Access for Agent Users, page 9-10.
Restricted Access User Role	Use this dropdown menu to specify a user role for users who accept restricted network access instead of installing the Cisco NAC Agent or installing and launching the Cisco NAC Web Agent.
Restricted Access Button Text	You can change the text in this box to show users who can log in to the Cisco NAC Appliance system a "customized" button in the Agent login dialog process.

Table 1-1 Agent Login—General Setup Configuration Options (continued)

Control	Description
Show Network Policy to NAC Agent and Cisco NAC Web Agent users (Windows only) [Network Policy Link:]	Click this checkbox if you want to display a link in the Agent login session to a Network Policy (Acceptable Use Policy) web page to Agent users. You can use this option to provide a policies or information page that users must accept before they access the network. This page can be hosted on an external web server or on the Clean Access Manager itself. • To link to an externally-hosted page, type the URL in the **Network Policy Link** field, in the format `https://mysite.com/helppages`. • To put the network policy page on the CAM, for example "helppage.htm," upload the page using **Administration > User Pages > File Upload**, then point to the page by typing the URL `https://<CAS_IP_address>/auth/helppage.htm` in the **Network Policy Link** field. **Note** The Network Policy page is only shown to the first user that logs in with the device. This helps to identify the authenticating user who accepted the Network Policy Page. Clearing the device from the Certified Devices List will force the user to accept the Network Policy again at the next login. For more details, see Figure 10-27 on page 10-20 and Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 9-11.
Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs (for Windows & In-Band setup, for OOB setup when OOB Logoff is enabled)	Click this option to enable logoff of the Agent from the Cisco NAC Appliance network when a user logs off the Windows domain (Start > Shutdown > Log off current user) or shuts down a Windows workstation. This removes the user from the Online Users list. **Note** If you do not enable the **Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs** option on the CAM, the last authenticated user remains logged in even if the current user on the client logs off from the client system. For SSO, the next user to use that client will be logged in with the credentials of the previous user. In the case of the Cisco NAC Web Agent (which does not perform SSO), the next user has the access level of the previous user. **Note** If a user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example), and the **Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs** option has not been enabled, the client machine remains in the Temporary role until the Session Timer expires and the user is given the opportunity to perform login/remediation again.
Refresh Windows domain group policy after login (for Windows only)	Click this checkbox to automatically refresh the Windows domain group policy (perform GPO update) after the user login (for Windows only). This feature is intended to facilitate GPO update when Windows AD SSO is configured for Cisco NAC Agent users. See the "Enable GPO Updates" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for more details.
Automatically close login success screen after [] secs	Click this checkbox and set the time to configure the Login success dialog to close automatically after the user is successfully certified/logged into normal login role (otherwise user has to click **OK** button). Setting the time to 0 seconds prevents display of the Agent Login success screen. Valid range is 0-300 seconds.
Automatically close logout success screen after [] secs (for Windows only)	Click this checkbox and set the time to configure the Logout success dialog to close automatically when the user manually logs out (otherwise user has to click **OK** button). Setting the time to 0 seconds prevents display of the logout success screen. Valid range is 0-300 seconds.

Web Login

Figure 1-3 Web Login—General Setup


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Web Login · Agent Login
User Role
Role2
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
Link to User Agreement Page Configuration Form
Show Network Scanner User Agreement page to web login users
Enable pop-up scan vulnerability reports from User Agreement page
Require users to be certified at every web login
Exempt certified devices from web login requirement by adding to MAC filters
Block/Quarantine users with vulnerabilities in role:
Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of:
quarantine role
Update
Cancel
183648

Web login users see the login and logout pages, quarantine role or blocked access pages and Nessus scan vulnerability reports, if enabled. You can also configure a User Agreement Page that appears to web login users before accessing the network.

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the initial Web Login session may feature extra authentication challenge-response dialogs beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager or Clean Access Server. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session.

Note Ensure that your RADIUS server and associated clients are configured to interact correctly according to the RADIUS authentication method you choose.

Table 1-2 explains the **General Setup > Web Login** configuration options shown in Figure 1-3. For examples and descriptions of web login user pages, see Table 1-3 on page 1-18.

Table 1-2 Web Login—General Setup Configuration Options

Control	Description
User Role	Choose the user role for which to apply Cisco NAC Appliance General Setup controls. The dropdown list shows all roles in the system. Configure user roles from **User Management > User Role** (see Adding a New User Role, page 6-7.)
Operating System	Choose the client OS for the specified user role. By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.

Table 1-2 Web Login—General Setup Configuration Options (continued)

Control	Description
Show Network Scanner User Agreement Page to web login users	Click this checkbox to present the **User Agreement Page** ("Virus Protection Information") after web login and network scanning. The page displays the content you configure in the **User Agreement** configuration form. Users must click the **Accept** button to access the network. **Note** The User Agreement page is only shown to the first user that logs in with the device. This helps to identify the authenticating user who accepted the UAP. Clearing the device from the Certified Devices List will force the user to accept the UAP again at the next login. If choosing this option, be sure to configure the page as described in Customize the User Agreement Page, page 12-19.
Enable pop-up scan vulnerability reports from User Agreement Page	Click this checkbox to enable web login users to see the results of their network scan from a popup browser window. If popup windows are blocked on the client computer, the user can view the report by clicking the **Scan Report** link on the Logout page.
Require users to be certified at every web login	• Click this checkbox to force user to go through network scanning every time they access the network. • If disabled (default), users only need to be certified the first time they access the network, or until their MAC address is cleared from the **Certified Devices List**. **Note** This option only applies to the In-Band Online Users list. When this option is enabled and the Online Users list entry is deleted, the corresponding Certified Devices List entry is deleted if there are no other Online Users list (either In-Band or Out-of-Band) entries with the same MAC address.
Exempt certified devices from web login requirement by adding to MAC filters	Click this checkbox to place the MAC address of devices that are on the Cisco NAC Appliance **Certified Devices List** into the authentication passthrough list. This allows devices to bypass authentication and posture assessment the next time they access the network.
Block/Quarantine users with vulnerabilities in role	• Click this checkbox and select a **quarantine** role from the dropdown menu to put the user in the quarantine role if found with vulnerabilities after network scanning. If quarantined, the user must correct the problem with their system and go through network scanning again until no vulnerabilities are found in order to access the network. • Click this checkbox and select **Block Access** from the dropdown menu to block the user from the network if found with vulnerabilities after network scanning. If a user is blocked, the Blocked Access page is shown with the content entered in the **Message (or URL) for Blocked Access Page:** field. **Note** The role session expiration time appears in parentheses next to the quarantine role name. This session time will also appears on the User Agreement Page, if display of the page is enabled for a quarantined user.
Show quarantined users the User Agreement Page of	If **Quarantine** is selected for **Block/Quarantine users with vulnerabilities in role**, this option appears below. It lets you present a User Agreement Page specific to the quarantine role chosen for users who fail scanning. Alternatively, Cisco NAC Appliance can present the page associated with the user's normal login role, or no page. See Customize the User Agreement Page, page 12-19 for further information.
Message (or URL) for Blocked Access Page:	If **Block Access** is selected for "**Block/Quarantine users with vulnerabilities in role**", this option appears. To modify the default message, type HTML text or enter a URL for the message that should appear when a user is blocked from the network for failing Nessus Scanning.

Client Posture Assessment Overview

Cisco NAC Appliance compliance policies reduce the threat of computer viruses, worms, and other malicious code on your network. Cisco NAC Appliance is a powerful tool that enables you to enforce network access requirements, detect security threats and vulnerabilities on clients, and distribute patches, antivirus and anti-spyware software. It lets you block access or quarantine users who do not comply with your security requirements, thereby stopping viruses and worms at the edge of the network, before they can do harm.

Cisco NAC Appliance evaluates a client system when a user tries to access the network. Almost all aspects of Cisco NAC Appliance are configured and applied by user role and operating system. This allows you to customize Cisco NAC Appliance as appropriate for the types of users and devices that will be accessing your network. Cisco NAC Appliance provides three different methods for finding vulnerabilities on client systems and allowing users to fix vulnerabilities or install required packages:

- Cisco NAC Appliance Agent only (Cisco NAC Agent or Cisco NAC Web Agent)
- Network scanning only
- Agent with network scanning

Summary Steps for Configuring Client Posture Assessment

The general summary of steps to configure client posture assessment in Cisco NAC Appliance is as follows:

Step 1 **Download Updates**.
Retrieve general updates for the Agent(s) and other deployment elements. See Retrieving Cisco NAC Appliance Updates, page 9-12.

Step 2 **Configure Agent-based access or network scanning per user role and OS in the General Setup tab**. Require use of the Agent for a role, enable network scanning web pages for web login users, and block or quarantine users with vulnerabilities. See Client Login Overview, page 1-6.

Step 3 **Configure the client posture assessment-related user roles with session timeout and traffic policies (In-Band)**. Traffic policies for the quarantine role allow access to the User Agreement Page and web resources for quarantined users who failed network scanning. Traffic policies for the Agent Temporary role allow access to the resources from which the user can download required software packages. See Configure Policies for Agent Temporary and Quarantine Roles, page 8-19.

Step 4 **Configure Agent-based posture assessment, network scanning, or both**.

- **If configuring Agent Login**. Require use of the Agent for the user role in the **General Setup > Agent Login** tab. Plan and define your requirements per user role. Configure AV Rules or create custom rules from checks. Map AV Rules to an AV Definition Update requirement, and/or map custom rules to a custom requirement (File Distribution/Link Distribution/Local Check). Map requirements to each user role. See Configuring Agent-Based Posture Assessment, page 9-39.
- **If configuring network scanning**. Load Nessus plugins to the Clean Access Manager repository. To enable network scanning, select the Nessus plugins to participate in scanning, then configure scan result vulnerabilities for the user roles and operating systems. Customize the User Agreement page. See Network Scanning Implementation Steps, page 12-3. Note that the results of network scanning may vary due to the prevalence of personal firewalls which block any network scanning from taking place.

Note The Cisco NAC Agent does not support Nessus-based network scanning.

Step 5 **Test your configurations** for user roles and operating systems by connecting to the untrusted network as a client. Monitor the Certified Devices List, Online Users page, and Event Logs during testing. Test network scanning by performing web login, checking the network scanning process, the logout page, and the associated client and administrator reports. Test the Agent by performing the initial web login and Agent download, login, Requirement checks and scanning, and view the associated client and administrator reports.

Step 6 If needed, manage the Certified Devices List by configuring other devices, such as floating or exempt devices. Floating devices must be certified at the start of every user session. Exempt devices are always excluded from Network Scanning (Nessus scans). See Manage Certified Devices, page 11-10.

For more information, see:

- Configuring Agent-Based Posture Assessment, page 9-39
- Network Scanning Implementation Steps, page 12-3

Cisco NAC Appliance Agents

Cisco NAC Agent

The Cisco NAC Agent provides local-machine Agent-based posture assessment and remediation for both 32- and 64-bit Windows operating systems and supports “double-byte” character formats that, along with full UTF-8 compliance, enable the you to offer native client-side localization for a number of common languages. (For a list of supported languages, see Cisco NAC Agent XML Configuration File Settings, page 9-23.) Users must download and install the Agent, which allows for visibility into the host registry, process checking, application checking, and service checking. The Agent can be used to perform AV/AS definition updates, distribute files uploaded to the Clean Access Manager, or distribute links to websites in order for users to fix their systems.

Note There is no client firewall restriction with Cisco NAC Agent posture assessment. The Agent can check client registry, services, and applications even if a personal firewall is installed and running.

Cisco NAC Agent client machine login and session behavior is determined by settings specified in the **NACAgentCFG.xml** Agent configuration file, residing in the install directory on the client machine. (The default install directory on Windows XP is **C:\Program Files\Cisco\Cisco NAC Agent**. However, you or the client machine user may specify a different directory.) You can customize the settings in the **NACAgentCFG.xml** file according to the parameters outlined in Cisco NAC Agent XML Configuration File Settings, page 9-23, or you can let the Cisco NAC Agent construct its own Agent configuration XML file using default settings.

The Cisco NAC Agent provides the following support:

- Easy download and installation of the Agent on the client via initial one-time web login. The Agent installs by default for the current user and all other users on the client PC.
- Posture assessment support for both 32- and 64-bit Windows operating systems (prior releases of Cisco NAC Appliance only provided authentication support for 64-bit Windows operating systems)

- "Double-byte" character support that enables the Agent to display user dialogs for supported locales/language OS platforms
- Evolution Data Optimized (EVDO) connections where no wired or wireless NICs are enabled on the client machine. For more information on enabling this function for the Cisco NAC Agent, see Table 9-10 "Client-Side MAC Address Management".
- Auto-upgrade. Once the Agent is installed on a client, it can automatically detect, download, and upgrade itself to next version. The Agent checks for an Agent update at every login request. The administrator can configure Agent auto-upgrade to be mandatory or optional for all users, or can disable update notification altogether.
- Built-in AV/AS checking support for major antivirus (AV) and antispyware (AS) vendors. AV/AS Rule and Requirement configuration facilitates the most common type of checking administrators need to perform on clients and allows the Agent to automatically detect and update AV and AS definition files on the client machine. AV/AS product support is kept up-to-date on the CAM through the use of Cisco NAC Appliance Updates, page 1-6.
- Ability to launch qualified/digitally signed executable programs when a client fails a requirement. See Configuring a Launch Programs Requirement, page 9-85 for details.
- Custom rule and check configuration. Administrators can configure requirements to check clients for specific applications, services, or registry entries using pre-configured Cisco checks and rules or by creating their own custom checks and rules.
- Multi-hop Layer 3 In-Band (IB) and Out-of-Band (OOB) deployment support and VPN concentrator/Layer 3 access. You can configure the CAM/CAS/Agent to enable clients to discover the CAS when the network configuration puts clients one or more Layer 3 hops away from the CAS (instead of in L2 proximity). Single Sign-On (SSO) is also supported when Cisco NAC Appliance is integrated (In-Band) behind Cisco VPN concentrators. For details, see "Enable L3 Deployment Support," "Integrating with Cisco VPN Concentrators," or "Configuring Layer 3 Out-of-Band (L3 OOB)" in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.
- Windows Domain Active Directory Single Sign-On. When Windows AD SSO is configured for the Cisco NAC Appliance, users with the Agent already installed can automatically log into Cisco NAC Appliance when they log into their Windows domain. The client system will be automatically scanned for requirements with no separate Agent login required. See the "Configuring Active Directory Single Sign-On (AD SSO)" chapter in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

Note Users logging into Cisco NAC Appliance via AD SSO must be running Windows Vista or Windows 7 and have the appropriate Cisco NAC Agent (version 4.7.1.15, 4.8.0.32, or 4.9.0.33) installed on their client machine in order to remain FIPS-compliant. Windows XP clients performing AD SSO do not conform to FIPS 140-2 compliance requirements.

- Automatic DHCP Release/Renew. When the Agent is used for login in OOB deployments, the Agent automatically refreshes the DHCP IP address if the client needs a new IP address in the Access VLAN. See DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6 for details.

Note For information on Access to Authentication VLAN change detection for an OOB client machine, see Configure Access to Authentication VLAN Change Detection, page 3-67.

- Cisco NAC Agent logoff with Windows logoff/shutdown. Administrators can enable or disable the Agent to log-off from the Cisco NAC Appliance network when a user logs off the Windows domain or shuts down a Windows machine. This feature does not apply to OOB deployments.

For complete details on the Agent configuration features mentioned above, see Chapter 9, "Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment."

For details on the features of each version of the Agent, see "Cisco NAC Appliance Agents" in the latest Release Notes.

Cisco NAC Web Agent

Unlike the Cisco NAC Agent, the Cisco NAC Web Agent is not a "persistent" entity, thus it only exists on the client machine long enough to accommodate a single user session. Instead of downloading and installing an Agent application, once the user opens a browser window, logs in to the NAC Appliance web login page, and chooses to launch the temporal Cisco NAC Web Agent, an ActiveX control or Java applet (you specify the preferred method using the **Web Client (ActiveX/Applet)** option in the **Administration > User Pages > Login Page** configuration page) initiates a self-extracting Agent installer on the client machine to install Agent files in a client's temporary directory, perform posture assessment/scan the system to ensure security compliance, and report compliance status back to the NAC Appliance system. During this period, the user is granted access only to the Temporary Role and if the client machine is not compliant for one or more reasons, the user is informed of the issues preventing network access and may do one of the following:

- Users must manually remediate/update their client machine and try to test compliance again before the Temporary Role times out
- Accept "restricted" network access for the time being and try to ensure the client machine meets requirements for the next login session

Note If an OOB user accepts restricted access, they remain in that role for as long as it is defined on the CAM. Therefore, even if the user is able to perform manual remediation while connected using the restricted access role, the client machine is not Re-Scanned until the session terminates and the user tries to log in again.

Note The Cisco NAC Web Agent does not perform client remediation. Users must adhere to NAC Appliance requirement guidelines independent of the Web Agent session to ensure compliance before they can gain access to the internal network. If users are able to correct/update their client machine to be compliant before the Temporary Role time-out expires, they can choose to "Re-scan" the client machine and successfully log in to the network.

Once the user has provided appropriate login credentials and the Web Agent ensures the client machine meets the NAC Appliance security requirements, the browser session remains open and the user is logged in to the network until the user clicks the **Logout** button in the Web Agent browser window, shuts off their system, or the NAC Appliance administrator terminates the session from the CAM. After the session terminates, the web interface logs the user out of the network, removes the session from the client machine, and the user ID disappears from the Online Users list.

Mac OS X Agent

Like the Cisco NAC Agent for windows client machines, provides local-machine Agent-based posture assessment and remediation for Macintosh client machines.

The Mac OS X Agent provides the following support:

- Easy download and installation of the Agent on the client via initial one-time web login. The Agent installs by default for the current user and all other users on the client machine.
- The Mac OS X Agent only performs a subset of the client posture assessment and remediation functions available to Windows users running the Cisco NAC Agent or Cisco NAC Web Agent. For more information, see Configuring Agent-Based Posture Assessment, page 9-39.
- Auto-upgrade. Once the Agent is installed on a client, it can automatically detect, download, and upgrade itself to next version. The Agent checks for a new update file at every login request. The administrator can configure Agent auto-upgrade to be mandatory or optional for all users, or can disable update notification altogether.
- Built-in AV/AS checking support for major antivirus (AV) and antispyware (AS) vendors. AV/AS Rule and Requirement configuration facilitates the most common type of checking administrators need to perform on clients and allows the Agent to automatically detect and update AV and AS definition files on the client machine. AV/AS product support is kept up-to-date on the CAM through the use of Cisco NAC Appliance Updates, page 1-6.

Note For information on Access to Authentication VLAN change detection for an OOB client machine, see Configure Access to Authentication VLAN Change Detection, page 3-67.

For complete details on the Agent configuration features mentioned above, see Chapter 9, "Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment."

For details on the features of each version of the Agent, see the latest Release Notes.

Clean Access Agent

(Persistent Agent option for Windows client machines available in releases of Cisco NAC Appliance prior to Release 4.6(1).)

For details on the Windows version of the Clean Access Agent, refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

Network Scanner

Note **Nessus-based network scanning capabilities only apply to web login users and Clean Access Agent users for whom a combination of client network scanning and Agent login functionality has been configured. The Cisco NAC Agent does not support Nessus-based network scanning.**

The Cisco NAC Appliance Network Scanner method provides network-based vulnerability assessment and web-based remediation. The network scanner in the local Clean Access Server performs the actual network scanning and checks for well-known port vulnerabilities to which a particular host may be prone. If vulnerabilities are found, web pages configured in the Clean Access Manager can be pushed to users to distribute links to websites or information on how users can fix their systems.

Network scans are implemented with Nessus plugins. Nessus (http://www.nessus.org) is an open-source vulnerability scanner. Nessus plugins check client systems for security vulnerabilities over the network. If a system is scanned and is found to be vulnerable or infected, Cisco NAC Appliance can take immediate action by alerting vulnerable users, blocking them from the network, or assigning them to a quarantine role in which they can fix their systems.

Note If a personal firewall is installed on the client, network scanning will most likely respond with a timeout result. You can decide how to treat the timeout result by quarantining, restricting, or allowing network access (if the personal firewall provides sufficient protection) to the client machine.

As new Nessus plugins are released, they can be loaded to your Clean Access Manager repository. Plugins that you have loaded are automatically published from the CAM repository to the Clean Access Servers, which perform the actual scanning. The CAM distributes the plugin set to the Clean Access Servers as they start up, if the CAS version of the plugin set differs from the CAM version.

Agent checking and network scanning can be coordinated, so that the Agent checks for software to fix vulnerabilities prior to network scanning. For example, if a Microsoft Windows update is required to address a vulnerability, you can specify it as a required package in the Agent. This allows the Agent to help users pass network vulnerability scanning before it is performed.

Note

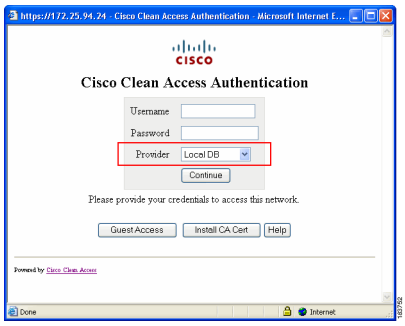
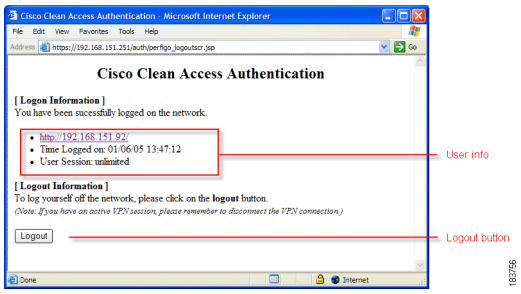
- You can use Nessus 2.2 plugins to perform scans in Cisco NAC Appliance. The filename of the uploaded Nessus plugin archive must be **plugins.tar.gz**. Cisco NAC Appliance software releases are shipped with Nessus version 2.2.7 only. Nessus version 2.2.7 has a NASL_LEVEL value of less than 3004. Cisco NAC appliance does not support Nessus plugins which require the NASL_LEVEL to be equal to or greater than 3004. Cisco NAC Appliance currently does not support Nessus version 3 plugins due to vendor licensing restrictions.
- Due to a licensing requirement by Tenable, Cisco is no longer able to bundle pre-tested Nessus plugins or automated plugin updates to Cisco NAC Appliance, effective Release 3.3.6/3.4.1. Customers can still download Nessus plugins selectively and manually through the Nessus site. For details on available plugins, see http://www.nessus.org/plugins/index.php?view=all.
  For details on Nessus plugin feeds, see http://www.nessus.org/plugins/index.php?view=feed.
- Cisco recommends using no more than 5-8 plugins for network scanning of a client system. More plugins can cause the login time to be long if the user has a firewall, as each plugin will have to timeout.

Table 1-3 summarizes the web pages that appear to users during the course of login and perform Nessus Scanning, and lists where they are configured in the web admin console.

Table 1-3 Web Login User Page Summary

Page	Configured in:	Purpose
Web Login Pages		

Table 1-3 Web Login User Page Summary (continued)

Page	Configured in:	Purpose
Login Page	**Administration > User Pages > Login Page** See User Login Page, page 5-1 for details.	The Login page is configured separately from web pages for Agent/network scanning, and is the network authentication interface when using network scanning only. Agent users only need to use it once to initially download the Agent installation file. Login pages can be configured per VLAN, subnet and client OS. The user enters his/her credentials to authenticate, and the CAM determines the user's role assignment based on local user/user role configuration. 
Logout Page (web login users only)	**User Management > User Roles > New Role or Edit Role** See Specify Logout Page Information, page 5-16 for details.	The Logout page appears only for users that use web login to authenticate. After the user successfully logs in, the Logout page pops up in its own browser and displays user status based on the combination of options you select.  **Note** Users (especially users in a quarantine role) should be careful not to close the Logout page to be able to log themselves out instead of having to wait for a session timeout.

For additional information on redirecting users by role to specific pages or URLs (outside of Cisco NAC Appliance), see Create Local User Accounts, page 6-15.

For additional Cisco NAC Appliance configuration information, see Configure General Setup, page 12-9.

For additional details on configuring Agent Requirements, see Configuring Agent-Based Posture Assessment, page 9-39.

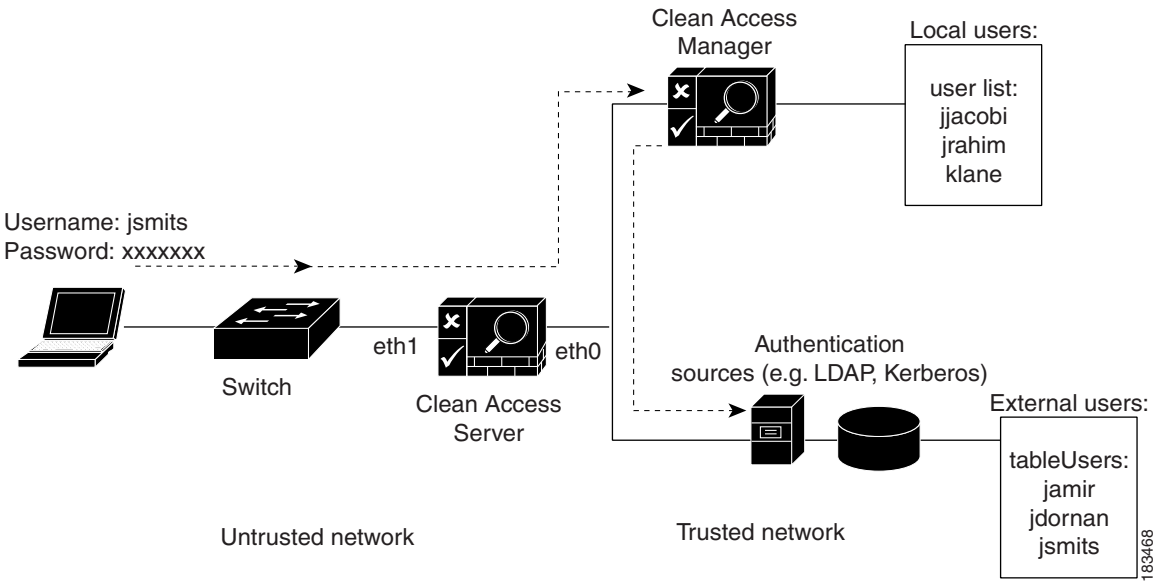
For complete details, see Chapter 12, "Configuring Network Scanning."

Managing Users

The Clean Access Manager makes it easy to apply existing authentication mechanisms to users on the network (Figure 1-4). You can customize user roles to group together and define traffic policies, bandwidth restrictions, session duration, client posture assessment, and other policies within Cisco NAC Appliance for particular groups of users. You can then use role-mapping to map users to these policies based on VLAN ID or attributes passed from external authentication sources.

When the Clean Access Server receives an HTTP request from the untrusted network, it checks whether the request comes from an authenticated user. If not, a customizable secure web login page is presented to the user. The user submits his or her credentials securely through the web login page, which can then be authenticated by the CAM itself (for local user testing) or by an external authentication server, such as LDAP, RADIUS, Kerberos, or Windows NT. If distributing the Agent, users download and install the Agent after the initial web login, then use the Agent after that for login/posture assessment.

Figure 1-4 Authentication Path



You can configure and impose posture assessment and remediation on authenticated users by configuring requirements for the Agent and/or network port scanning.

Note The Cisco NAC Web Agent performs posture assessment, but does not provide a medium for remediation. The user must manually fix/update the client machine and "Re-Scan" to fulfill posture assessment requirements with the Web Agent.

With IP-based and host-based traffic policies, you can control network access for users before authentication, during posture assessment, and after a user device is certified as "clean."

With IP-based, host-based, and (for Virtual Gateway deployments) Layer 2 Ethernet traffic policies, you can control network access for users before authentication, during posture assessment, and after a user device is certified as "clean."

Note Layer 2 Ethernet traffic control only applies to Clean Access Servers operating in Virtual Gateway mode.

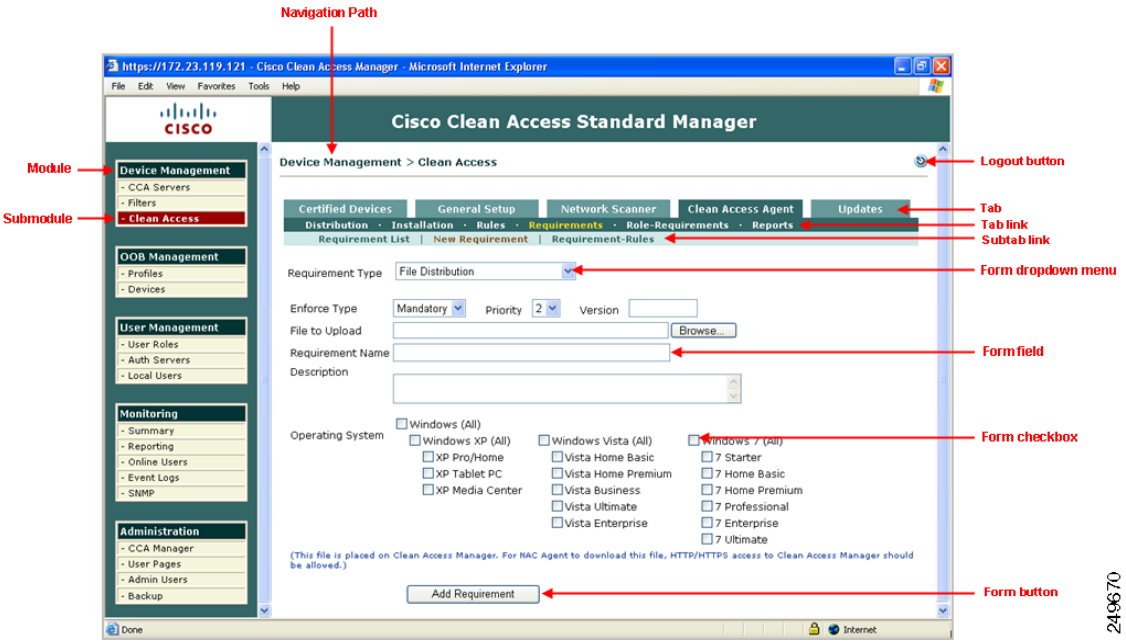
Finally, you can monitor user activity from the web console through the Online Users page (for L2 and L3 deployments) and the Certified Devices List (L2 deployments only).

Overview of Web Admin Console Elements

Note Administrators using Internet Explorer Version 6 to access a FIPS 140-2 compliant CAM/CAS web console must ensure that TLSv1 (which is disabled by default in Microsoft Internet Explorer Version 6) is enabled in the browser Advanced settings in order to "talk" to the network. See the "Enabling TLSv1 on Internet Explorer Version 6" installation troubleshooting section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Once the Cisco NAC Appliance software is enabled with a license, the web admin console of the CAM provides an easy-to-use interface for managing Cisco NAC Appliance deployment. The left panel of the web console displays the main modules and submodules. The navigation path at the top of the web console indicates your module and submodule location in the interface. Clicking a submodule opens the tabs of the interface, or in some cases configuration pages or forms directly. Configuration pages allow you to perform actions, and configuration forms allow you to fill in fields. Web admin console pages can comprise the following elements shown in Figure 1-5 on page 1-21.

Figure 1-5 Web Admin Console Page Elements



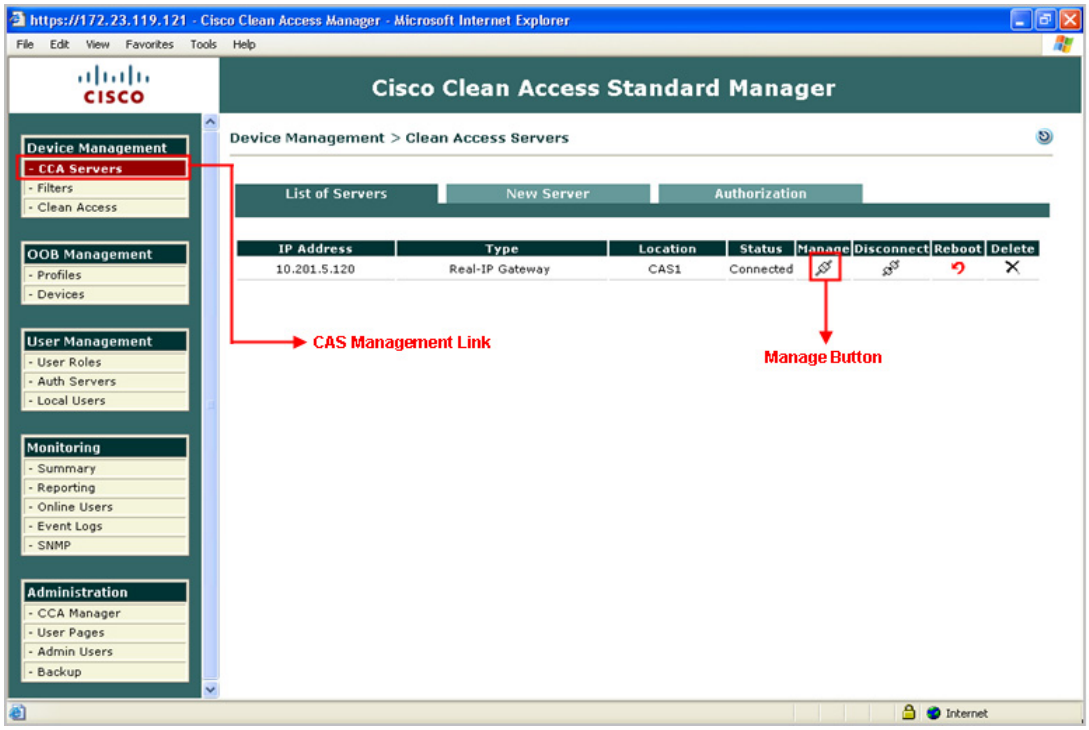
Note This document uses the following convention to describe navigational links in the admin console: **Module > Submodule > Tab > Tab Link > Subtab link** (if applicable)

Clean Access Server (CAS) Management Pages

The Clean Access Server must be added to the Clean Access Manager domain before it can be managed from the web admin console. Chapter 2, "Device Management: Adding Clean Access Servers, Adding Filters," explains how to do this. Once you have added a Clean Access Server, you access it from the admin console as shown in the steps below. In this document, "*CAS management pages*" refers to the set of pages, tabs, and forms shown in Figure 1-7.

1. Click the **CCA Servers** link in the **Device Management** module. The **List of Servers** tab appears by default.

Figure 1-6 CAS List of Servers Page

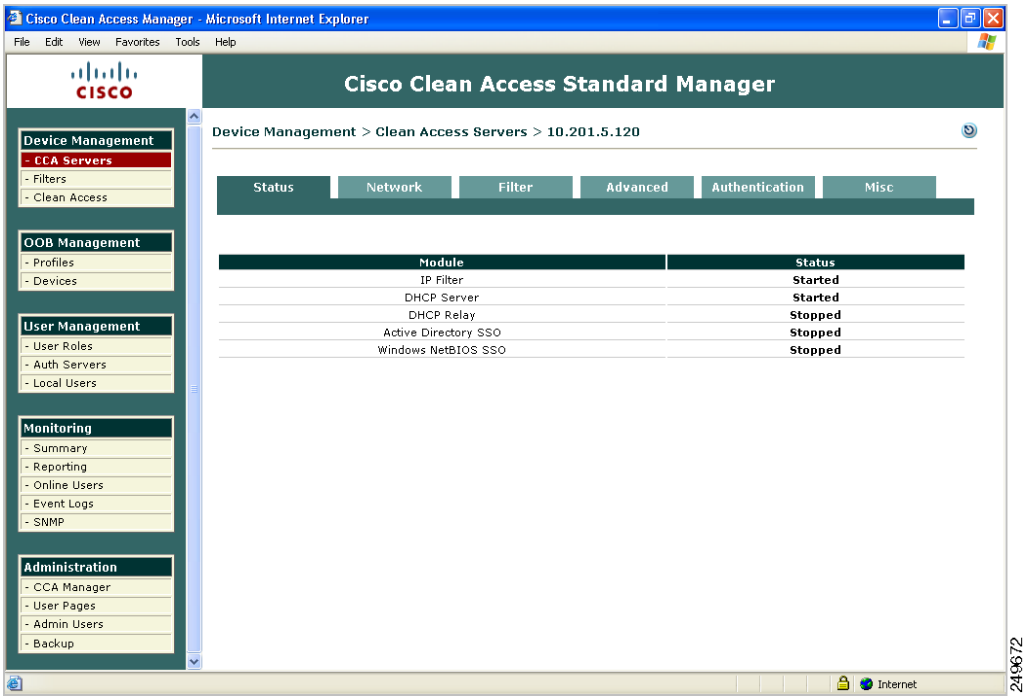


2. Click the **Manage** icon for the IP address of the Clean Access Server you want to access.

Note For high-availability Clean Access Servers, the Service IP is automatically listed first, and the IP address of the currently active CAS is shown in brackets.

3. The CAS management pages for the Clean Access Server appear as shown in Figure 1-7.

Figure 1-7 CAS Management Pages



Publishing Information

The Clean Access Manager publishes the configuration settings to the Clean Access Servers whenever the following scenarios happen:

- A new CAS is added to the CAM.
- Connection between CAM and CAS restores after a communication failure between them.
- CAM boots up.
- CAS boots up.
- When CAM failover happens, the newly Active CAM would publish configuration to all connected CASs.

Admin Console Summary

Table 1-4 summarizes the major functions of each module in the web admin console.

Table 1-4 Summary of Modules in Clean Access Manager Web Admin Console

Module	Module Description
	The **Device Management** module allows you to: • Add, configure, manage, and perform software upgrade on Clean Access Servers via the CAS management pages (shown in Figure 1-7). See Chapter 2, "Device Management: Adding Clean Access Servers, Adding Filters". For details on local CAS configuration including AD SSO, DHCP, and Cisco VPN Concentrator integration, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*. For upgrade information, see the "Upgrading" section of the corresponding *Release Notes for Cisco NAC Appliance*. • Configure device or subnet filters to allow devices on the untrusted side to bypass authentication and posture assessment. See Global Device and Subnet Filtering, page 2-10 for details. • Configure posture assessment (Agent/network scanning) and/or remediation per user role and OS. See: – Configuring Agent-Based Posture Assessment, page 9-39 – Chapter 12, "Configuring Network Scanning" **Note** User sessions are managed by MAC address (if available) or IP address, as well as the user role assigned to the user, as configured in the **User Management** module.
	The **OOB Management** module is used for Cisco NAC Appliance Out-of-Band deployment. It allows you to: • Configure Out-of-Band Group, Switch, WLC, and Port profiles, as well as the Clean Access Manager's SNMP Receiver. • Add supported Out-of-Band switches, configure the SNMP traps sent, manage individual switch ports via the **Ports** (and **Port Profile**) page and monitor the list of Discovered Clients. See Chapter 3, "Switch Management: Configuring Out-of-Band Deployment"

Table 1-4 Summary of Modules in Clean Access Manager Web Admin Console (continued)

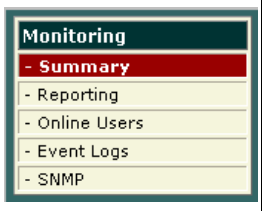
Module	Module Description
	The **User Management** module allows you to: • Create normal login user roles to associate groups of users with authentication parameters, traffic control policies, session timeouts, and bandwidth limitations. If using role-based configuration for OOB Port Profiles, you can configure the Access VLAN via the user role. • Add IP and host-based traffic control policies to configure network access for all the user roles. Configure traffic policies/session timeout for the Agent Temporary role and Quarantine role(s) to limit network access if a client device fails requirements or is found to have network scanning vulnerabilities. • Add Auth Servers to the CAM (configure external authentication sources on your network). • Add auth sources such as Active Directory SSO and Cisco VPN SSO to enable Single Sign-On (SSO) when the CAS is configured for AD SSO or Cisco VPN Concentrator integration. • Create complex mapping rules to map users to user roles based on LDAP or RADIUS attributes, or VLAN IDs. • Perform RADIUS accounting. • Create local users authenticated internally by the CAM (for testing) For details see: – Chapter 6, "User Management: Configuring User Roles and Local Users" – Chapter 7, "User Management: Configuring Authentication Servers" – Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" For additional details on Cisco VPN Concentrator integration, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.
	The **Monitoring** module allows you to: • View a status summary of your deployment. • View the current system information and preset reports. • Manage In-Band and Out-of-Band online users. • View, search, and redirect Clean Access Manager event logs. • Configure basic SNMP polling and alerting for the Clean Access Manager See Chapter 13, "Monitoring Event Logs".

Table 1-4 Summary of Modules in Clean Access Manager Web Admin Console (continued)

Module	Module Description
	The **Administration** module allows you to: • Configure Clean Access Manager network and high availability (failover) settings. See the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)* for detailed information. • Configure CAM SSL certificates, system time, CAM /CAS product licenses, create or restore CAM database backup snapshots, and download technical support logs See Chapter 14, "Administering the CAM" • Perform software upgrade on the CAM See the "Upgrading to a New Software Release" section of the corresponding *Release Notes for Cisco NAC Appliance*. • Add the default login page (mandatory for all user authentication), and customize the web login page(s) for web login users. See Chapter 5, "Configuring User Login Page and Guest Access". • Configure multiple administrator groups and access privileges. See Admin Users, page 14-47.



Device Management: Adding Clean Access Servers, Adding Filters

This chapter describes how to add and manage Clean Access Servers from the Clean Access Manager and configure device and/or subnet filters. It contains the following sections.

- Working with Clean Access Servers, page 2-2
- Global and Local Administration Settings, page 2-8
- Global Device and Subnet Filtering, page 2-10
- Integrating Cisco ISE Profiler, page 2-29

The first step in implementing Cisco NAC Appliance is configuring devices in the Clean Access Manager (CAM)'s administrative domain. Clean Access Servers must be added to the CAM in order to manage them directly in the web console.

By default, Cisco NAC Appliance forces user devices on the untrusted side of the CAS to authenticate when attempting to access the network.

User roles, user authentication, user web pages, and traffic policies for In-Band user traffic must be configured for users on the untrusted network as described in the following chapters:

- Chapter 6, "User Management: Configuring User Roles and Local Users"
- Chapter 7, "User Management: Configuring Authentication Servers"
- Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule"

If deploying Cisco NAC Appliance for Out-of-Band, you will also need to configure the CAM as described in Chapter 3, "Switch Management: Configuring Out-of-Band Deployment".

After Cisco NAC Appliance is configured for user traffic on the unstrusted side of your network, you may need to allow devices on the untrusted side to **bypass** authentication and posture assessment (for example printers or VPN concentrators). See Global Device and Subnet Filtering, page 2-10 for how to configure filters in the Clean Access Manager for these kinds of devices.

Working with Clean Access Servers

The Clean Access Server gets its runtime parameters from the Clean Access Manager and cannot operate until it is added to the CAM's domain. Once the CAS is installed and added to the CAM, you can configure local parameters in the CAS and monitor it through the web admin console.

This section describes the following:

- Add Clean Access Servers to the Managed Domain
- Manage the Clean Access Server
- Configure Clean Access Manager-to-Clean Access Server Authorization
- Check Clean Access Server Status
- Disconnect a Clean Access Server
- Reboot the Clean Access Server
- Remove the Clean Access Server from the Managed Domain
- Troubleshooting when Adding the Clean Access Server

Note In order to establish the initial secure communication channel between a CAM and CAS, you must import the root certificate from each appliance into the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.

For details on configuring local CAS-specific settings, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Add Clean Access Servers to the Managed Domain

The Clean Access Server must be running to be added to the Clean Access Manager.

Note If intending to configure the Clean Access Server in Virtual Gateway mode (IB or OOB), you must disable or unplug the untrusted interface (eth1) of the CAS until after you have added the CAS to the CAM from the web admin console. Keeping the eth1 interface connected while performing initial installation and configuration of the CAS for Virtual Gateway mode can result in network connectivity issues.

For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**.

See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

To add a Clean Access Server:

Step 1 From **Device Management**, click the **CCA Servers** link on the navigation menu.



Step 2 Click the **New Server** tab.

Figure 2-1 Add New Server



Step 3 In the **Server IP address** field, type the IP address of the Clean Access Server's eth0 trusted interface.

Note The eth0 IP address of the CAS is the same as the Management IP address.

Step 4 Optionally, in the **Server Location** field, type a description of the Clean Access Server's location or other identifying information.

Step 5 For In-Band operation, choose one of the following operating modes for the Clean Access Server from the **Server Type** list:

- **Virtual Gateway** – Operates as an L2 transparent bridge, while providing IPSec, filtering, virus protection, and other services.
- **Real-IP Gateway** – Acts as the default gateway for the untrusted network.

Step 6 For Out-of-Band operation, you must choose one of the following Out-of-Band operating types:

- **Out-of-Band Virtual Gateway**—Operates as a Virtual Gateway during authentication and certification, before the user is switched Out-of-Band (i.e., the user is connected directly to the access network).
- **Out-of-Band Real-IP Gateway**—Operates as a Real-IP Gateway during authentication and certification, before the user is switched Out-of-Band (i.e., the user is connected directly to the access network).

The CAM can control both In-Band and Out-of-Band Clean Access Servers in its domain. However, the CAS itself must be **either** In-Band or Out-of-Band.

For more information on Out-of-Band deployment, see Chapter 3, "Switch Management: Configuring Out-of-Band Deployment."

See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for further details on the CAS operating modes.

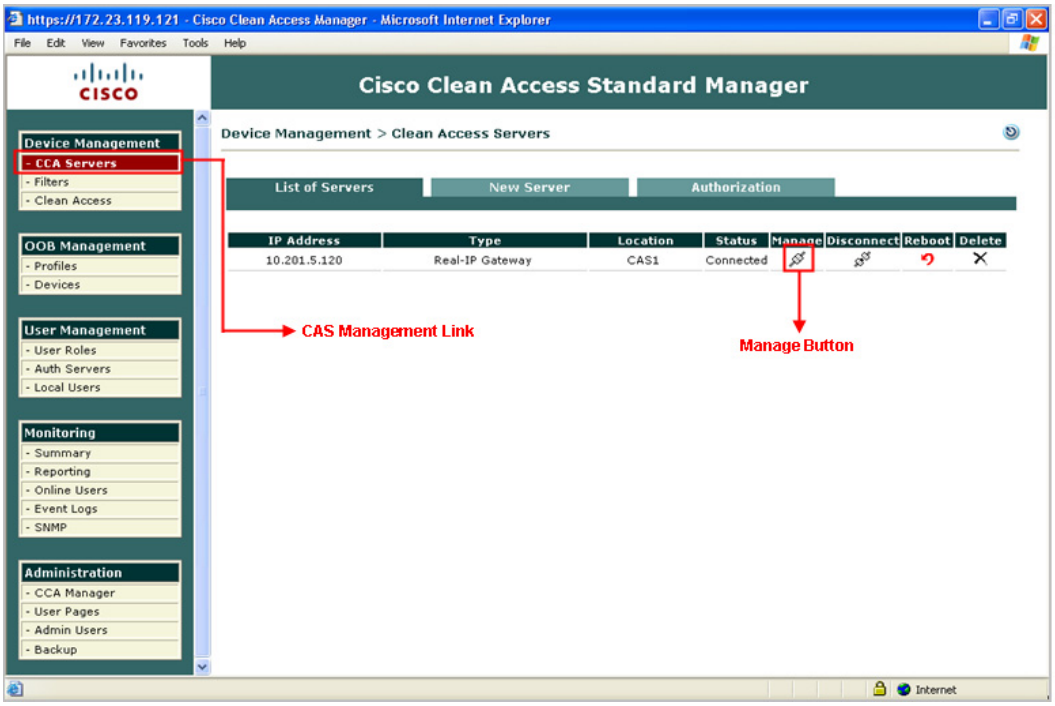
Step 7 Click **Add Clean Access Server**. The Clean Access Manager looks for the Clean Access Server on the network, and adds it to its list of managed Servers (Figure 2-2). The Clean Access Server is now in the Clean Access Manager's administrative domain.

Manage the Clean Access Server

After adding the Clean Access Server, you can configure CAS-specific settings such as VLAN Mapping or DHCP configuration. For some parameters, such as traffic control policies, the settings in the CAS can override the CAM's global settings.

Once you add the CAS to the Clean Access Manager, the CAS appears in the **List of Servers** tab as one of the managed Servers, as shown in Figure 2-2.

Figure 2-2 List of Servers Tab



Each Clean Access Server entry lists the IP address, server type, location, and connection status of the CAS. In addition four management control icons are displayed: **Manage**, **Disconnect**, **Reboot**, and **Delete**.

Click the **Manage** icon to administer the Clean Access Server.

Note For more information on configuring Clean Access Servers (such as DHCP or high availability) see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Configure Clean Access Manager-to-Clean Access Server Authorization

When you add Clean Access Servers to the CAM, you can also choose to enable mutual Authorization between the appliances to enhance network security.

Using the CAM Authorization web console page, administrators can enter the Distinguished Names (DNs) of one or more CASs to ensure secure communications between the CAM and CAS(s). Once you enable the Authorization feature and add one or more CASs to the Authorized CCA Servers list, the CAM does not accept communications from CASs that do not appear in the list. Therefore, when you choose to employ and enable this feature in your network, you must add *all* of your managed CASs to the Authorized CCA Servers list to ensure you maintain CAM-CAS connection for all of the CASs in your network.

Likewise, you must also enable this feature and specify a CAM DN on all of the CASs in your network to establish two-way authorization between the CAMs/CASs.

If you have deployed your CAMs/CASs in an HA environment, you can enable authorization for both the HA-Primary and HA-Secondary machines in the HA pair by specifying the DN of only the HA-Primary appliance. For example, if the CAM manages a CAS HA pair, you only need to list the HA-Primary CAS on the CAM's Authorization page. Likewise, if you are enabling this feature on a CAS managed by a CAM HA pair, you only need to list the HA-Primary CAM on the CAS's Authorization page.

Summary of Steps to Configure Clean Access Manager-to-Clean Access Server Authorization

Step 1 Configure CAS Authorization on the CAM web console under **Device Management > Clean Access Servers > Authorization** (see Enable Authorization and Specify Authorized Clean Access Servers, page 2-6).

Step 2 Configure CAM Authorization on the CAS web console under **Administration > Authorization** (see the "Enable Authorization and Specify the Authorized Clean Access Manager" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*).

Step 3 Before deploying in a production environment, obtain trusted CA-signed certificates for CAM and CAS and import them to CAM/CAS under **Administration > SSL > Trusted Certificate Authorities** (for CAM), and **Administration > SSL > Trusted Certificate Authorities** (for CAS).

Warning **If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.5 and later. You must correct your certificate chain to successfully upgrade to release 4.5 and later. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

Step 4 If you are upgrading your Cisco NAC Appliance release, clean up Trusted Certificate Authorities on the CAM under **Administration > CCA Manager > SSL > Trusted Certificate Authorities**, and on the CAS under **Administration > SSL > Trusted Certificate Authorities** (see Manage Trusted Certificate Authorities, page 14-16 and the "View and Remove Trusted Certificate Authorities" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*, respectively).

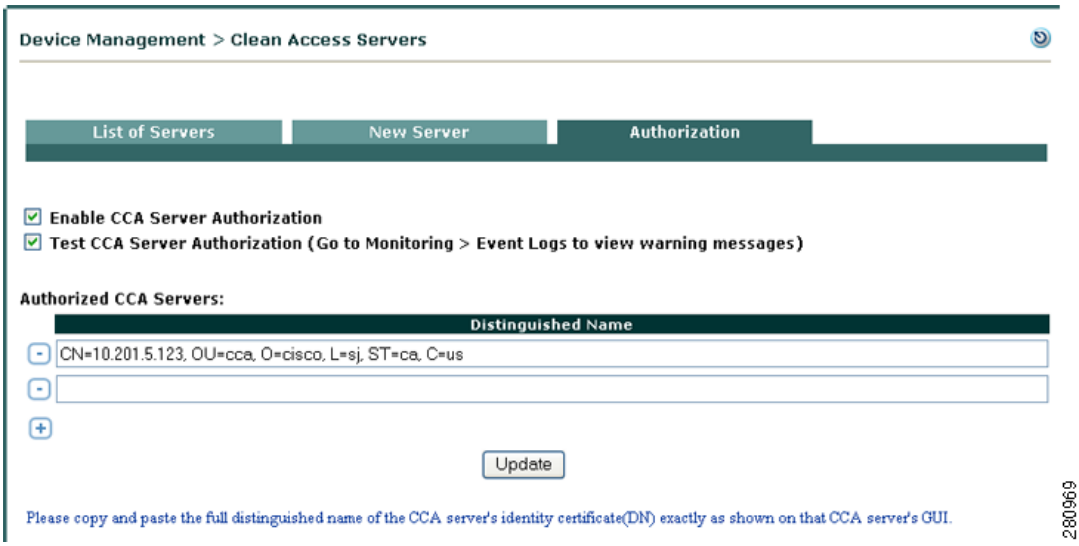
Note If you use the Authorization feature in a CAM HA-pair, follow the guidelines in Backing Up and Restoring CAM/CAS Authorization Settings, page 14-62 to ensure you are able to *exactly* duplicate your Authorization settings from one CAM to its high availability counterpart.

Enable Authorization and Specify Authorized Clean Access Servers

To enable authorization and specify CASs authorized to communicate with the CAM:

Step 1 Go to **Device Management > Clean Access Servers > Authorization** (Figure 2-3).

Figure 2-3 Device Management > Clean Access Servers > Authorization


Device Management > Clean Access Servers
List of Servers
New Server
Authorization
Enable CCA Server Authorization
Test CCA Server Authorization (Go to Monitoring > Event Logs to view warning messages)
Authorized CCA Servers:
Distinguished Name
CN=10.201.5.123, OU=cca, O=cisco, L=sj, ST=ca, C=us
Update
Please copy and paste the full distinguished name of the CCA server's identity certificate(DN) exactly as shown on that CCA server's GUI.
280969

Step 2 Click **Enable CCA Server Authorization** to turn on the Cisco NAC Appliance authorization feature.

Warning **Do not click the Enable CCA Server Authorization option without also entering one or more full distinguished names of CASs you want to authorize to communicate securely with the CAM. If you enable this feature and have not specified any CAS distinguished names, you will not be able to communicate with any of the CASs in your network.**

Step 3 Click the plus icon "+" and enter the full distinguished name of a CAS you want to authorize to communicate securely with the CAM. For example, enter a text string like "CN=110.21.5.123, OU=cca, O=cisco, L=sj, ST=ca, C=us" in the Distinguished Name field.

Note Distinguished names require exact syntax. Therefore, Cisco recommends copying the CAS DN from the top of the list of entries in the **Administration > SSL > X509 Certificate** CAS web console page and pasting it into the CAM's Authorization page to ensure you specify the exact name for the CAS on the CAM.

Step 4 If you want to first test whether or not the CAM is able to authorize and connect to the CAS(s) in your network, click **Test CCA Server Authorization** to test connection with the CASs you include in the Authorized CCA Servers list. The CAM generates SSL Connection log messages that you can view in the CAM **Monitoring > Event Logs** web console page after you click **Update** in step 5.

Step 5 Click **Update** to ensure the CAS(s) you have added become part of the group of servers authorized to communicate back-and-forth with the CAM.

When you click **Update**, the CAM restarts services between the CAM and all CASs in the Authorized CCA Server list, which may cause brief network interruptions to users logged into the Cisco NAC Appliance system.

- If you enabled the **Test CCA Server Authorization** option and there are one or more Clean Access Servers in the Authorized CCA Server list to which the CAM is unable to connect, warning (yellow flag) messages appear in the event log.
- If you did not enable the **Test CCA Server Authorization** option and there are one or more Clean Access Servers in the Authorized CCA Server list to which the CAM is unable to connect, error (red flag) messages appear in the event log.

See View Logs, page 13-4 for more information.

Check Clean Access Server Status

The operational status of each Clean Access Server appears in the **Status** column:

- **Connected**—The CAM can reach the CAS successfully.
- **Not connected**—The CAS is rebooting, or the network connection between the CAM and CAS is broken.

If the Clean Access Server has a status of **Not connected** unexpectedly (that is, it is not down for standard maintenance, for example), try clicking the **Manage** icon to force a connection attempt. If successful, the status changes to **Connected**. Otherwise, check for a connection problem between the CAM and CAS and make sure the CAS is running. If necessary, try rebooting the CAS.

Note The Clean Access Manager monitors the connection status of all configured Clean Access Servers. The CAM will try to connect a disconnected CAS every 3 minutes.

Disconnect a Clean Access Server

When a Clean Access Server is disconnected, it displays **Not Connected** status but remains in the Clean Access Manager domain. You can always click **Manage** to connect the CAS and configure it.

Additionally, if at any point the Clean Access Server is out of sync with the Clean Access Manager, you can disconnect the Clean Access Server then reconnect it. The Clean Access Manager will again publish the data configured for the Clean Access Server and keep the CAS in sync.

In contrast, if you delete the Clean Access Server, all secondary configuration settings are lost.

Reboot the Clean Access Server

You can perform a graceful reboot of a Clean Access Server by clicking the **Reboot** icon in the **List of Servers** tab. In a graceful reboot, the Clean Access Server performs all normal shutdown procedures before restarting, such as writing logging data to disk.

Remove the Clean Access Server from the Managed Domain

Deleting a Clean Access Server in the **List of Servers** tab removes it from the List of Servers and the system. To remove a Clean Access Server, click the **Delete** icon next to the CAS. In order to reuse a Clean Access Server that you have deleted, you have to re-add it to the Clean Access Manager.

Note that when the Clean Access Server is removed, any secondary configuration settings specific to the CAS are deleted. Secondary settings are settings that are *not* configured at installation time or through the `service perfigo config` script, and include policy filters, traffic routing, and encryption parameters.

Settings that *are* configured at installation time, such as interface addresses, are kept on the Clean Access Server and are restored if the CAS is later re-added to the CAM's administrative domain.

Removing an active CAS has the following effect on users accessing the network through the CAS at the time it is deleted:

- If the CAS and CAM are connected when the CAS is deleted, the network connections for active users are immediately dropped. Users are no longer able to access the network. (This is because the CAM is able to delete the CAS's configuration immediately, so that the IP addresses assigned to active users are no longer valid in relation to any security policies applicable to the CASs.) New users will be unable to log into the network.
- If the connection between the CAS and CAM is broken at the time the CAS is deleted, active users will be able to continue accessing the network until the connection is reestablished. This is because the CAM cannot delete the CAS's configuration immediately. New users will be unable to log into the network.

Troubleshooting when Adding the Clean Access Server

See "Troubleshooting when Adding the Clean Access Server" in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for troubleshooting details.

Global and Local Administration Settings

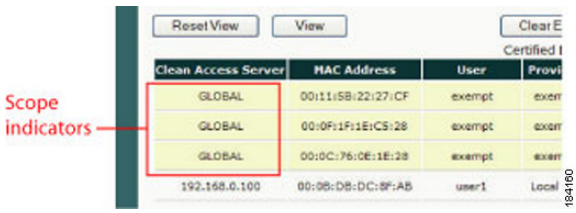
The CAM web admin console has the following types of settings:

- **Clean Access Manager administration settings** are relevant only to the CAM itself. These include its IP address and host name, SSL certificate information, and High-Availability (failover) settings.
- **Global administration settings** are set in the Clean Access Manager and pushed from the CAM to **all** Clean Access Servers. These include authentication server information, global device/subnet filter policies, user roles, and Cisco NAC Appliance configuration.

- **Local administration settings** are set in the CAS management pages for a Clean Access Server and apply only to that CAS. These include CAS network settings, SSL certificates, DHCP and 1:1 NAT configuration, VPN concentrator configuration, IPSec key changes, local traffic control policies, and local device/subnet filter policies.

The global or local scope of a setting is indicated in the **Clean Access Server** column in the web admin console, as shown in Figure 2-4.

Figure 2-4 Scope of Settings



- **GLOBAL**—The entry was created using a global form in the CAM web admin console and applies to all Clean Access Servers in the CAM's domain.
- **<IP Address>**—The entry was created using a local form from the CAS management pages and applies only for the CAS with this IP address.

In general, pages that display global settings (referenced by GLOBAL) also display local settings (referenced by CAS IP address) for convenience. These local settings can usually be edited or deleted from global pages; however, they can only be **added** from the local CAS management pages for a particular Clean Access Server.

Global and Local Settings

Global (defined in CAM for all CASs) and local (CAS-specific) settings often coexist on the same CAS. If a global and local setting conflict, either the local setting overrides the global setting, or the priority of the policy determines which global or local policy to enforce.

- For device filter policies affecting a *range* of MAC addresses and traffic control policies, the priority of the policy (higher or lower in **Device Management > Filters > Devices > Order**) determines which global or local policy to enforce. Any device filter policy for an individual MAC address takes precedence over a filter policy (either global or local) for a range of addresses that includes the individual MAC address.
- For subnet filter policies where one subnet filter specifies a subset of an address range in a broader subnet filter, the CAM determines the priority of the filter based on the size of the subnet address range. The smaller the subnet (like a /30 or /28 subnet mask), the higher the priority in the subnet filter hierarchy.
- Some features must be enabled both on the CAS (via the CAS management pages) and/or configured in the CAM console, for example:
  - L3 support (for multi-hop L3 deployments) is enabled per CAS, but may require login page/Agent configuration on CAM
  - Bandwidth Management is enabled per CAS but can be configured for all roles on the CAM
  - Active Directory SSO is configured per CAS but requires Auth Provider on CAM
  - Cisco VPN Concentrator SSO is configured per CAS but requires Auth Provider on CAM

- Agent requirements and network scanning plugins are configured globally from the CAM and apply to all CASs.

Global Device and Subnet Filtering

This section describes the following:

- Overview
- Device Filters and User Count License Limits
- Adding Multiple Entries
- Corporate Asset Authentication and Posture Assessment by MAC Address
- Device Filters for In-Band Deployment
- Device Filters for Out-of-Band Deployment
- Device Filters for Out-of-Band Deployment Using IP Phones
- In-Band and Out-of-Band Device Filter Behavior Comparison
- Device Filters and Gaming Ports
- Global vs. Local (CAS-Specific) Filters
- Global Device Filter Lists from Cisco NAC Profiler
- Configure Device Filters
- Configure Subnet Filters

Overview

By default, Cisco NAC Appliance forces user devices on the untrusted side of the CAS to authenticate (log in) when attempting to access the network. If you need to allow devices on the untrusted side to **bypass** authentication, you can configure device or subnet filters.

Filter lists (configured under **Device Management > Filters**) can be set by MAC, IP, or subnet address, and can automatically assign user roles to devices. Filters allow devices (user or non-user) to bypass both authentication and (optionally) posture assessment. This section describes how to configure device and subnet filters.

Device filters are specified by MAC address (and optionally IP for In-Band deployments) of the device, and can be configured for either In-Band (IB) or Out-of-Band (OOB) deployments. The MAC addresses are input and authenticated through the CAM, but the CAS is the device that performs the actual filtering action. For OOB, the use of device filters must also be enabled in the Port Profile (see Add Port Profile, page 3-34). For both IB and OOB, devices put in the filter list bypass authentication. In both Layer 2 and Layer 3 deployments, Out-of-Band device filters rely only on client MAC address when determining whether or not to act upon MAC notification messages from an associated switch. (Device filters do not take client IP addresses into account for Out-of-Band client machines because the CAM cannot reliably verify Out-of-Band client IP addresses.)

Subnet filters can be configured for IB deployments only and are specified by subnet address and subnet mask (in CIDR format).

You can configure device or subnet filters to do the following:

- IB: Bypass login/posture assessment and allow all traffic for the device/subnet.
  OOB: Bypass login/posture assessment and assign the Default Access VLAN to the device.

- IB: Block network access to the device/subnet.
  OOB: Block network access and assign the Auth VLAN to the device.
- IB: Bypass login/posture assessment and assign a user role to the device/subnet.
  OOB: Bypass login/posture assessment and assign the Out-of-Band User Role VLAN to the device (the Access VLAN configured in the user role).

Note Because a device in a Filter entry is allowed/denied access without authentication, the device will not appear in the Online Users list in a Layer 2 deployment. (They can, however, still be tracked on the In-Band network through the Active Layer 2 Device Filters List.) See View Active Layer 2 Device Filter Policies, page 2-26 for more information.

Some uses of device filters include:

- For printers on user VLANs, you can set up an “allow” device filter for the printer's MAC address to allow the printer to communicate with Windows servers. Cisco recommends configuring device filters for printers in OOB deployment also. This prevents a user from connecting to a printer port in order to bypass authentication.
- For In-Band Cisco NAC Appliance L3/VPN concentrator deployment, you can configure a device or subnet filter to allow traffic from an authentication server on the trusted network to communicate with the VPN concentrator on the untrusted network.
- For very large numbers of non-NAC network devices (IP phones, printers, fax machines, etc.), you can add them to the device filter list to ensure they bypass Cisco NAC Appliance authentication, posture assessment, and remediation functions.

Note Device filter lists can also be automatically created and updated on the CAM using Cisco NAC Profiler. See Global Device Filter Lists from Cisco NAC Profiler, page 2-18 for details.

Note The Policy Sync feature exports all global device filters created on the Master CAM to the Receiver CAMs. Any MAC address which is in the Master CAM’s global Device Filter list will be exported, including Cisco NAC Profiler generated filters. See Policy Import/Export, page 14-28 for details.

Note Device filter settings and/or subnet filter settings take precedence over the CAS Fallback Policy. While in CAS fallback mode, CAS device filter settings determine behavior based on the client MAC address. If device filter settings do not apply (for example, if the CAS is a Layer 3 gateway and cannot determine the client MAC address), the CAS also looks for applicable subnet filter settings before applying the CAS Fallback Policy. See *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

Note In wireless deployments, when you are adding a client to the filter list, make sure that the client is not connected to the WLC and authenticated by NAC. If the client machine is already connected to WLC and authenticated, adding it to the filter list does not work. You need to disconnect the client machine and reconnect it to enable the filter.

Device Filters and User Count License Limits

- MAC addresses specified with the "ALLOW" option in the Device Filter list (bypass authentication/posture assessment/remediation) **do not** count towards the user count license limit.
- MAC addresses specified with the "CHECK" option in the Device Filter list (bypass authentication but go through posture assessment/remediation) **do** count towards the user count license limit.

Note The maximum number of (non-user) devices that can be filtered is based on memory limitations and is not directly connected to user count license restrictions. A CAS can safely support approximately 5,000 MAC addresses per 1 GB of memory.

Device filters and user/endpoint count license limits related to Cisco NAC Profiler depend upon the Cisco NAC Profiler system deployment. For specific information, see *Cisco NAC Appliance Service Contract / Licensing Support* and *Cisco NAC Profiler Installation and Configuration Guide*.

Changing the behavior of MAC address role-based device filters is not dynamic, it is mandate for CAM to receive link-up/MAC notification in case of wired and Association/ Disassociation trap in case of wireless to avoid first time posture assessment when NAC agent pop-up is closed at the end-client.

Adding Multiple Entries

You can enter a large number of MAC addresses into the device filter list by:

1. Specifying wildcards and MAC address ranges when configuring device filters.
2. Copying and pasting individual MAC addresses (one per line) into the New Device Filter form and adding all of them with one click.
3. Using the API (cisco_api.jsp) **addmac** function to add the MAC addresses programmatically. See API Support, page 14-65 for details.

Note You can automate the management of large number of endpoints by deploying the Cisco NAC Profiler solution. When configured, the Cisco NAC Profiler Server/Collector automatically populates and maintains global device filters on the CAM for profiled endpoints. See Global Device Filter Lists from Cisco NAC Profiler, page 2-18 for more information.

Corporate Asset Authentication and Posture Assessment by MAC Address

Cisco NAC Appliance can perform MAC-based authentication and posture assessment of client machines without requiring the user to log into Cisco NAC Appliance. This feature is implemented through the "CHECK" device filter control for global and local device filters and the Agent. The Cisco NAC Web Agent performs posture assessment, but does not provide a medium for remediation. The user must manually fix/update the client machine and "Re-Scan" to fulfill posture assessment requirements with the Web Agent.

Note The CHECK feature only applies to Cisco NAC Appliance Agents which support posture assessment.

The following Device Filter configuration options are available:

- **CHECK** and **IGNORE** device filter options.
- **ROLE** and **CHECK** filters require choosing a **User Role** from the dropdown menu.
- **IGNORE** is for OOB only. For IB, checking this option has no effect.
- **IGNORE** is for global filters only. It does not appear on CAS New/Edit filter pages.
- **IGNORE** device filters are intended to replace "allow" device filters that were specified for IP phones in previous releases.

Note Administrators should reconfigure their device filters for IP phones to use the **IGNORE** option in order to avoid creating unnecessary MAC notification traps. For more information, see Device Filters for Out-of-Band Deployment Using IP Phones, page 2-15.

Device filter policies have different applicability in L2 deployments (deployments where the CAS is in L2 proximity to the end points/user devices) versus L3 deployments (where the CAS may be one or more hops away from the end points/user devices). Note that in an L3 deployment, the endpoint needs to access the network using a web browser (Java Applet/ActiveX) or the Agent for Cisco NAC Appliance to be able to obtain the end point's MAC address. The behavior in L2 and L3 deployments is different, as described in Table 2-1.

Table 2-1 CAM L2/L3 Device Filter Options

Option	L2	L3
ALLOW	Allows all traffic from the end-point - no authentication or posture assessment is required	Allows all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role - no authentication or posture assessment is required
DENY	Denies all traffic from the end-point	Denies all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role
ROLE	Allows traffic from the end-point without any authentication or posture assessment as specified by role traffic policies (for backward compatibility with Cisco NAC Appliance 3.x, this will continue to behave the same way)	Once MAC address is known, posture assessment is performed if configured following which traffic is allowed as per role traffic policies
CHECK	Performs posture assessment as specified for the Role following which traffic is allowed as per role traffic policies	(Same as above)
IGNORE	For OOB only - ignores SNMP traps from managed switch ports for the specified MAC address(es)	For OOB only - ignores SNMP traps from managed switch ports for the specified MAC address(es)

Note In both Layer 2 and Layer 3 deployments, Out-of-Band device filters rely only on client MAC address when determining whether or not to act upon MAC notification messages from an associated switch. (Device filters do not take client IP addresses into account for Out-of-Band client machines because the CAM cannot reliably verify Out-of-Band client IP addresses.)

Note When you are changing the behavior of the MAC address for **Role-Based** device filters, the change is not dynamic. The CAM should receive Linkup or MAC Notification in case of wired network. The CAM should receive Association/ Disassociation traps in case of wireless network. This is mandatory to avoid first time Posture Assessment when the NAC Agent popup is closed at the client end.

Device Filters for In-Band Deployment

Cisco NAC Appliance assigns user roles to users either by means of authentication attributes, or through device/subnet filter policies. As a result, a key feature of device/subnet filter policy configuration is the ability to assign a system user role to a specified MAC address or subnet. Cisco NAC Appliance processing uses the following order of priority for role assignment:

1. MAC address
2. Subnet/IP address
3. Login information (login ID, user attributes from auth server, VLAN ID of user machine, etc.)

Therefore, if a MAC address associates the client with "Role A," but the user's login ID associates him or her to "Role B," "Role A" is used.

For complete details on user roles, see Chapter 6, "User Management: Configuring User Roles and Local Users."

Note For more information on In-Band vs. Out-of-Band client machine behavior based on specified Device Filter type, see In-Band and Out-of-Band Device Filter Behavior Comparison, page 2-16.

Note For management of Access Points (APs) from the trusted side, you can ensure the APs are reachable from the trusted side (i.e. through SNMP, HTTP, or whatever management protocol is used) by configuring a filter policy through **Device Management > Filters > Devices**.

Device Filters for Out-of-Band Deployment

The Clean Access Manager respects the global Device Filters list for Out-of-Band deployments. As is the case for In-Band deployments, for OOB, the rules configured for MAC addresses on the global Device Filter list will have the highest priority for user/device processing. In both Layer 2 and Layer 3 deployments, Out-of-Band device filters rely only on client MAC address when determining whether or not to act upon MAC notification messages from an associated switch. (Device filters do not take client IP addresses into account for Out-of-Band client machines because the CAM cannot reliably verify Out-of-Band client IP addresses.)

For OOB, the order of priority for rule processing is as follows:

1. Device Filters (if configured with a MAC address, and if enabled for OOB)
2. Certified Devices List
3. Out-of-Band Online User List

MAC address device filters configured for OOB have the following options and behavior:

- **ALLOW**—Bypass login and posture assessment and assign **Default Access VLAN** to the port
- **DENY**—Bypass login and posture assessment and assign **Auth VLAN** to the port
- **ROLE**—Bypass login and L2 posture assessment and assign **User Role VLAN** to the port
- **CHECK**—Bypass login, apply posture assessment, and assign **User Role VLAN** to the port
- **IGNORE**—Ignore SNMP traps from managed switches (IP Phones)

Note

- To use global device filters for OOB, you must enable the **Change VLAN according to global device filter list** option for the Port Profile (under **OOB Management > Profiles > Port > New** or **Edit**). See Add Port Profile, page 3-34 for details.
- This feature applies to global device filters only. Cisco strongly recommends you do not configure any local (CAS-specific) device filters when deployed in an Out-of-Band environment.
- See Out-of-Band User Role VLAN, page 6-10 for details on VLAN assignment via the user role.

Note

- When you are changing the behavior of the MAC address device filters from **ALLOW** to **DENY**, the change is not dynamic. As the client traffic is directed to default Access VLAN initially, when the behavior changes to **DENY**, the traffic should be directed to Authentication VLAN. You should manually remove the MAC address from CDL/OUL to apply the **DENY** rule to that MAC address device filters.
- When you are changing the behavior of the MAC address device filters from **DENY** to **ALLOW**, the change is dynamic. When the client traffic reaches the eth1 interface of the CAS, it checks the Device filter rules and allows the user though the behavior has been moved from **Deny** to **ALLOW**.

Note For more information on In-Band vs. Out-of-Band client machine behavior based on specified Device Filter type, see In-Band and Out-of-Band Device Filter Behavior Comparison, page 2-16.

For further details, see Chapter 3, "Switch Management: Configuring Out-of-Band Deployment."

Device Filters for Out-of-Band Deployment Using IP Phones

You must create a Global Device filter list of MAC addresses designed to *ignore* IP phones through which client machines connect to your network. You can define a list of MAC addresses by compiling a collection of individual MAC addresses (Cisco recommends this method only for small deployments), specify a range of MAC addresses using range delimiters and/or wildcard characters, and you can also extract a list of MAC addressees from an existing IP phone management application like Cisco CallManager.

Once you build a list of the applicable IP phone MAC addresses, ensure that Cisco NAC Appliance *ignores* them by enabling the **Change VLAN according to global device filter list** option for the Port Profile (under **OOB Management > Profiles > Port > New** or **Edit**) when you configure your Cisco NAC Appliance system for OOB. This ensures that the IP phones MAC notification behavior cannot initiate a switch from one VLAN to another (from Access to Authentication VLAN, for example), thus inadvertently terminating the associated client machine's connection. See Configure OOB Switch Management on the CAM, page 3-25 for details.

In-Band and Out-of-Band Device Filter Behavior Comparison

VLAN assignments and whether or not the users appear in the Online Users list and associated client machines appear in the Certified Devices List differ depending on which filter type (ALLOW, DENY, ROLE, CHECK, or IGNORE) you configure. The following general guidelines apply when determining client traffic behavior for In-Band and Out-of-Band deployments:

- In-Band traffic is subject to both global and CAS-specific filter assignments, depending on the hierarchy defined in **Device Management > Filters > Devices > Order**.
- If the Port Profile has the **Change VLAN according to global device filter list** option enabled, the CAM directs the switch to follow global device filter configuration when assigning VLANs to ports.
- Out-of-Band client machines associated with a specific Port Profile are only governed by global device filters.

Table 2-2 Layer 2 and Layer 3 In-Band and Out-of-Band MAC Address FIlter Behavior

Device Filter Type	Layer 2 In-Band (Global and CAS)	Layer 3 In-Band (Global and CAS)	Out-of-Band without Port Profile option (Global)—Out-of-Band (CAS)	Out-of-Band with Port Profile option (Global only)
ALLOW	Allow traffic	Allow traffic (add Online Users list/Certified Devices List entries, no posture assessment)	Allow traffic in In-Band mode	Client traffic is directed to default Access VLAN
DENY	Deny traffic	Deny traffic once MAC address is known	Deny traffic in In-Band mode	Client traffic is directed to Authentication VLAN
ROLE	Put in role and apply role policies	Do posture assessment, add Online Users list/Certified Devices List entries, put in role and apply role policies	Put in role and apply role policies in In-Band mode	Client traffic is directed to Access VLAN (based on Port Profile)
CHECK (device in Certified Devices List)	Put in role and apply role policies (no Online Users list entry)	Do posture assessment, add Online Users list/Certified Devices List entries, put in role and apply role policies	Put in role and apply role policies in In-Band mode (no Online Users list entry)	Client traffic is directed to Access VLAN (based on Port Profile and no Online Users list entry)

Table 2-2 Layer 2 and Layer 3 In-Band and Out-of-Band MAC Address FIlter Behavior

Device Filter Type	Layer 2 In-Band (Global and CAS)	Layer 3 In-Band (Global and CAS)	Out-of-Band without Port Profile option (Global)—Out-of-Band (CAS)	Out-of-Band with Port Profile option (Global only)
CHECK (device *not* in Certified Devices List)	Do posture assessment (In-Band Online Users list entry in Temporary role) and add Certified Devices List entry after posture assessment (no Online Users list entry)	(Same as above)	Do posture assessment (In-Band Online Users list entry in Temporary role), add Certified Devices List entry after posture (Out-of-Band Online Users list entry) and assign to Access VLAN (based on Port Profile)	Do posture assessment (In-Band Online Users list entry in temp role), add Certified Devices List entry after posture (Out-of-Band Online Users list entry) and assign to Access VLAN (based on Port Profile)
IGNORE	No effect (normal behavior)	No effect (normal behavior)	No effect (normal behavior)	SNMP traps are ignored

The **Require users to be certified at every web login** option only applies to the In-Band Online Users list. When this option is enabled and the Online Users list entry is deleted, the corresponding Certified Devices List entry is deleted if there are no other Online Users list (either In-Band or Out-of-Band) entries with the same MAC address.

Device Filters and Gaming Ports

To allow gaming services, such as Microsoft Xbox Live, Cisco recommends creating a gaming user role and adding a filter for the device MAC addresses (under **Device Management > Filters > Devices > New**) to place the devices into that gaming role. You can then create traffic policies for the role to allow traffic for gaming ports. For additional details, see:

- Allowing Gaming Ports, page 8-24
- http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q16
- Adding a New User Role, page 6-7

Global vs. Local (CAS-Specific) Filters

You can add device/subnet filter policies at a global level for all Clean Access Servers in the Clean Access Manager **Filters** pages, or for a specific Clean Access Server through the CAS management pages. The CAM stores both types of access filters and distributes the global filter policies to all Clean Access Servers and the local filter policies to the relevant CAS.

For subnet filter policies (in **Device Management > Filters > Subnet**) where one subnet filter specifies a subset of an address range in a broader subnet filter, the CAM determines the priority of the filter based on the size of the subnet address range. The smaller the subnet (like a /30 or /28 subnet mask), the higher the priority in the subnet filter hierarchy. For example, a subnet filter policy allowing traffic from the 192.168.128.0/28 address range would take precedence over another subnet filter policy denying traffic from the from the 192.168.128.0/24 address range. Whether the subnet filter policy is global or local makes no difference when determining the priority.

For device filter policies specifying a range of MAC addresses where two or more policies potentially affect the same MAC address, the priority of the policy (in **Device Management > Filters > Devices > Order**) determines which global or local policy to enforce. However, any device filter specifying an individual MAC address takes precedence over a filter policy (either global or local) defining a range of addresses that includes the individual MAC address.

See Global and Local Administration Settings, page 2-8 for more information.

This section describes the forms and the steps to add global access filter policies. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for how to add local access filter policies.

Note The CAM prioritizes the global Device Filters list (not CAS-specific filters) for OOB deployments.

Global Device Filter Lists from Cisco NAC Profiler

To create and manage large numbers of non-user endpoint devices, such as network printers, IP phones, UPS devices, HVAC sensors, and wireless access controllers, you can deploy Cisco NAC Profiler. The Cisco NAC Profiler system enables you to automatically discover, categorize, and monitor hundreds or even thousands of endpoints for which user authentication and/or posture assessment does not apply.

The Cisco NAC Profiler solution consists of two primary components:

- **Cisco NAC Profiler Server**—The Cisco NAC Profiler Server manages the Cisco NAC Profiler Collector component enabled on each Clean Access Server. The Cisco NAC Profiler Server populates entries on the CAM's global device filter list (**Device Management > Filters > Devices > List**) for the endpoints it profiles and monitors. Clicking the Description link for a Profiler entry brings up the NAC Profiler Server's Endpoint Summary data right inside the CAM web console, as shown in Figure 2-5 and Figure 2-6. The Cisco NAC Profiler Server is configured and managed via its own web console interface, as described in the *Cisco NAC Profiler Installation and Configuration Guide*.
- **Cisco NAC Profiler Collector**—The Cisco NAC Profiler Collector is a service that can be enabled on a NAC-3310 or NAC-3350 Clean Access Server running Release 4.1(3) or later. You must purchase a Cisco NAC Profiler Server appliance and obtain and install Cisco NAC Profiler/Collector licenses on the Cisco NAC Profiler Server to deploy the Cisco NAC Profiler solution. See the "CLI Commands for Cisco NAC Profiler" section of the *Cisco NAC Appliance Hardware Installation Guide* for details.

Note Refer to the *Release Notes for Cisco NAC Profiler* for release compatibility information.

Figure 2-5 Cisco NAC Profiler Entries in CAM Device Filters

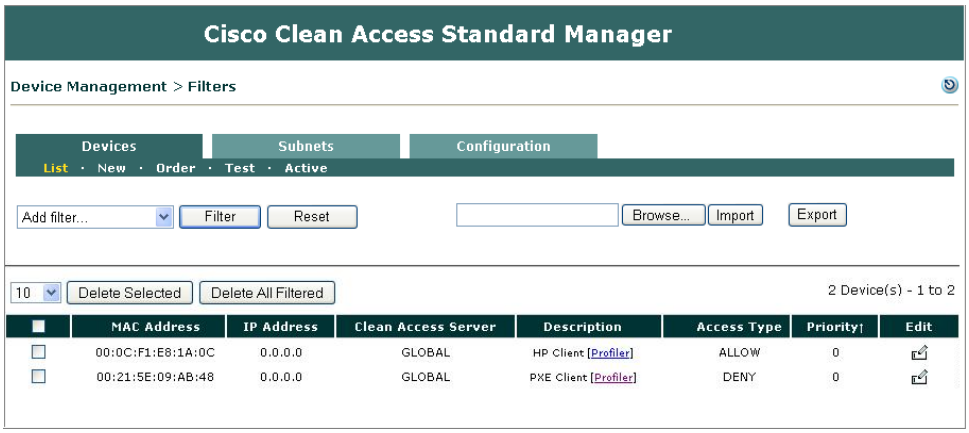
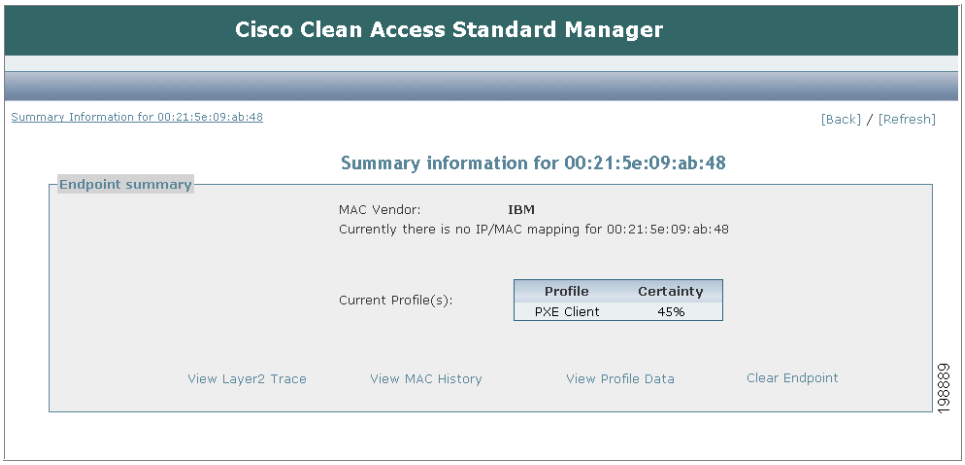


Figure 2-6 Endpoint Summary



Note The Policy Sync feature exports all global device filters created on the Master CAM to the Receiver CAMs. Any MAC address which is in the Master CAM's global Device Filter list will be exported, including Cisco NAC Profiler generated filters. See Policy Import/Export, page 14-28 for details.

Configure Device Filters

This section describes the following:

- Add Global Device Filter
- Display/Search/Import/Export Device Filter Policies
- Edit Device Filter Policies
- Delete Device Filter Policies

Add Global Device Filter

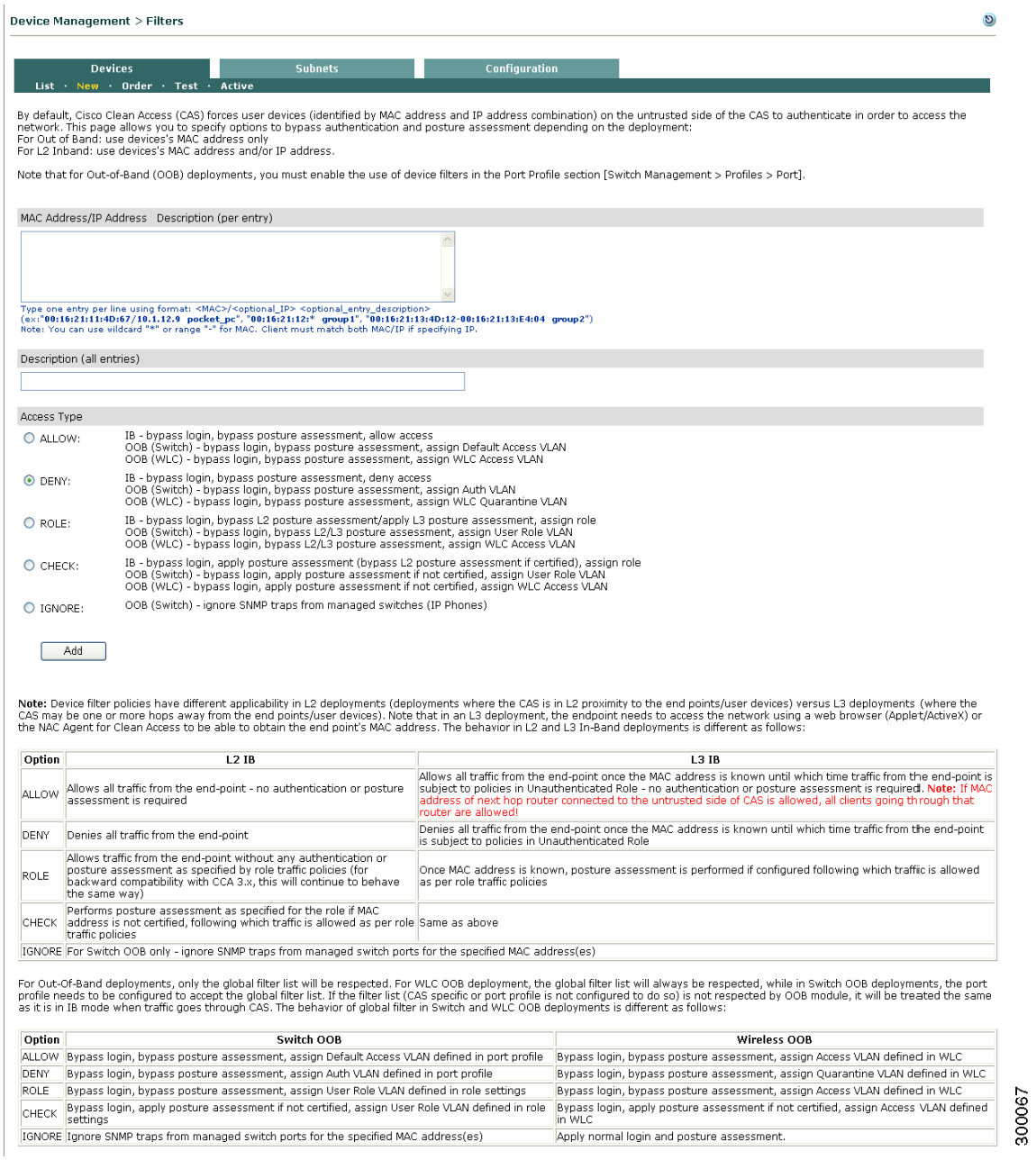
If there is a MAC address entry in the Device Filter list, the machine can also be checked per Cisco NAC Appliance policies (e.g., Agent-based checks, network scanner checks). The device is authenticated based on MAC address but will still have to go through scanning (network and/or Agent).

A device filter set up as described in the following steps applies across all Clean Access Servers in the CAM domain.

Note For more information on In-Band vs. Out-of-Band client machine behavior based on specified Device Filter type, see In-Band and Out-of-Band Device Filter Behavior Comparison, page 2-16.

Step 1 Go to **Device Management > Filters > Devices > New**.

Figure 2-7 New Device Filter


Device Management > Filters
Devices
Subnets
Configuration
List · New · Order · Test · Active
By default, Cisco Clean Access (CAS) forces user devices (identified by MAC address and IP address combination) on the untrusted side of the CAS to authenticate in order to access the network. This page allows you to specify options to bypass authentication and posture assessment depending on the deployment:
For Out of Band: use devices's MAC address only
For L2 Inband: use devices's MAC address and/or IP address.
Note that for Out-of-Band (OOB) deployments, you must enable the use of device filters in the Port Profile section [Switch Management > Profiles > Port].
MAC Address/IP Address Description (per entry)
Type one entry per line using format: <MAC>/<optional_IP> <optional_entry_description>
(ex:"00:16:21:11:4D:67/10.1.12.9 pocket_pc", "00:16:21:12:* group1", "00:16:21:13:4D:12-00:16:21:13:E4:04 group2")
Note: You can use wildcard "*" or range "-" for MAC. Client must match both MAC/IP if specifying IP.
Description (all entries)
Access Type
ALLOW: IB - bypass login, bypass posture assessment, allow access
OOB (Switch) - bypass login, bypass posture assessment, assign Default Access VLAN
OOB (WLC) - bypass login, bypass posture assessment, assign WLC Access VLAN
DENY: IB - bypass login, bypass posture assessment, deny access
OOB (Switch) - bypass login, bypass posture assessment, assign Auth VLAN
OOB (WLC) - bypass login, bypass posture assessment, assign WLC Quarantine VLAN
ROLE: IB - bypass login, bypass L2 posture assessment/apply L3 posture assessment, assign role
OOB (Switch) - bypass login, bypass L2/L3 posture assessment, assign User Role VLAN
OOB (WLC) - bypass login, bypass L2/L3 posture assessment, assign WLC Access VLAN
CHECK: IB - bypass login, apply posture assessment (bypass L2 posture assessment if certified), assign role
OOB (Switch) - bypass login, apply posture assessment if not certified, assign User Role VLAN
OOB (WLC) - bypass login, apply posture assessment if not certified, assign WLC Access VLAN
IGNORE: OOB (Switch) - ignore SNMP traps from managed switches (IP Phones)
Add
Note: Device filter policies have different applicability in L2 deployments (deployments where the CAS is in L2 proximity to the end points/user devices) versus L3 deployments (where the CAS may be one or more hops away from the end points/user devices). Note that in an L3 deployment, the endpoint needs to access the network using a web browser (Applet/ActiveX) or the NAC Agent for Clean Access to be able to obtain the end point's MAC address. The behavior in L2 and L3 In-Band deployments is different as follows:
Option | L2 IB | L3 IB
ALLOW | Allows all traffic from the end-point - no authentication or posture assessment is required | Allows all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role - no authentication or posture assessment is required. Note: If MAC address of next hop router connected to the untrusted side of CAS is allowed, all clients going through that router are allowed!
DENY | Denies all traffic from the end-point | Denies all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role
ROLE | Allows traffic from the end-point without any authentication or posture assessment as specified by role traffic policies (for backward compatibility with CCA 3.x, this will continue to behave the same way) | Once MAC address is known, posture assessment is performed if configured following which traffic is allowed as per role traffic policies
CHECK | Performs posture assessment as specified for the role if MAC address is not certified, following which traffic is allowed as per role traffic policies | Same as above
IGNORE | For Switch OOB only - ignore SNMP traps from managed switch ports for the specified MAC address(es)
For Out-Of-Band deployments, only the global filter list will be respected. For WLC OOB deployment, the global filter list will always be respected, while in Switch OOB deployments, the port profile needs to be configured to accept the global filter list. If the filter list (CAS specific or port profile is not configured to do so) is not respected by OOB module, it will be treated the same as it is in IB mode when traffic goes through CAS. The behavior of global filter in Switch and WLC OOB deployments is different as follows:
Option | Switch OOB | Wireless OOB
ALLOW | Bypass login, bypass posture assessment, assign Default Access VLAN defined in port profile | Bypass login, bypass posture assessment, assign Access VLAN defined in WLC
DENY | Bypass login, bypass posture assessment, assign Auth VLAN defined in port profile | Bypass login, bypass posture assessment, assign Quarantine VLAN defined in WLC
ROLE | Bypass login, bypass posture assessment, assign User Role VLAN defined in role settings | Bypass login, bypass posture assessment, assign Access VLAN defined in WLC
CHECK | Bypass login, apply posture assessment if not certified, assign User Role VLAN defined in role settings | Bypass login, apply posture assessment if not certified, assign Access VLAN defined in WLC
IGNORE | Ignore SNMP traps from managed switch ports for the specified MAC address(es) | Apply normal login and posture assessment.
300067

Step 2 In the **New** Device Filter form, enter the MAC address of the device(s) for which you want to create a policy in the text field. Type one entry per line using the following format:

```
<MAC>/<optional_IP> <optional_entry_description>
```

Note the following:

- You can use wildcards "*****" or a range "**-**" to specify multiple MAC addresses.
- Separate multiple devices with a return.

- As an option, you can enter an IP address with the MAC to make sure no one spoofs the MAC address to gain network access. If you enter both a MAC and an IP address, the client must match both for the rule to apply.
- You can specify a description by device or for all devices. A description specific to a particular device (in the MAC Address field) supersedes a description that applies all devices in the **Description (all entries)** field. There cannot be spaces within the description in the device entry (see Figure 2-7).

Step 3 Choose the policy for the device from the **Access Type** choices:

- **ALLOW**
  IB - bypass login, bypass posture assessment, allow access
  OOB - bypass login, bypass posture assessment, assign Default Access VLAN
- **DENY**
  IB - bypass login, bypass posture assessment, deny access
  OOB - bypass login, bypass posture assessment, assign Auth VLAN
- **ROLE**
  IB - bypass login, bypass L2 posture assessment, assign role
  OOB - bypass login, bypass L2 posture assessment, assign User Role VLAN. The Out-of-Band User Role VLAN is the Access VLAN configured in the user role. See Chapter 6, "User Management: Configuring User Roles and Local Users" for details.
- **CHECK**
  IB - bypass login, apply posture assessment, assign role
  OOB - bypass login, apply posture assessment, assign User Role VLAN
- **IGNORE**
  OOB (only) - ignore SNMP traps from managed switches (IP Phones)

Note For OOB, you must also enable the use of global device filters at the Port Profile level under **OOB Management > Profiles > Port > New** or **Edit**. See Add Port Profile, page 3-34 for details.

Step 4 Click **Add** to save the policy.

Step 5 The **List** page under the **Devices** tab appears.

The following examples are all valid entries (that can be entered at the same time):

```
00:16:21:11:4D:67/10.1.12.9 pocket_pc
00:16:21:12:* group1
00:16:21:13:4D:12-00:16:21:13:E4:04 group2
```

Note If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role. See Control Bandwidth Usage, page 8-13 for details.

Note Troubleshooting Tip: If you see ERROR: "Adding device MAC failed" and you are unable to add any devices in the filter list (regardless of which option is checked, or whether an IP address/description is included), check the Event Logs. If you see "xx:xx:xx:xx:xx:xx could not be added to the MAC list", this can indicate that one of the CASs is disconnected.

Display/Search/Import/Export Device Filter Policies

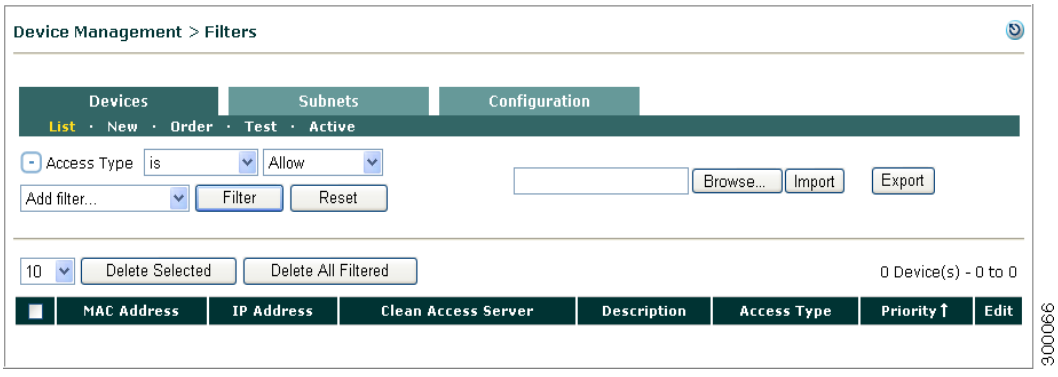
- Priorities can be defined for ranges (via the Order page).
- A single MAC address device filter (e.g. 00:14:6A:6B:6C:6D) always takes precedence on the filter List over a wildcard/range device filter (e.g. 00:14:6A:6B:*, or 00:14:6A:*).
- New wildcard/range device filters are always put at the end of the **List** page. To change the priority, go to the **Order** page.
- The role assignment for a single MAC address device filter always takes precedence over other filters. You can check the role assignment to be used for a MAC address using the **Test** page.
- The **Test** page shows which filter will take effect for the MAC address entered.

To filter the list of known devices:

Step 1 You can narrow the number of devices displayed in the filter list (under **Device Management > Filters > Devices > List)** using the following search criteria and respective modifiers available in the **Filter** dropdown list:

Filter Type	Modifier	Filter Entry
MAC Address	is, is not, contains, starts with, ends with	Any full or partial MAC address in format *AA*:*BB*:*CC*:*DD*:*EE*:*FF*
IP Address	is, is not, contains, starts with, ends with	Any full or partial IP address in format *A.B.C.D*
Clean Access Server	is, is not	(Dropdown menu options) **GLOBAL**, <*CAS_IP_address*>
Description	is, is not, contains, starts with, ends with	Any text string
Access Type	is, is not	(Dropdown menu options) **Allow**, **Deny**, **Role-Based**, **Check-Based**, **Ignore**
Priority	is, is not, contains, starts with, ends with	Any number

Figure 2-8 Device Filter List—Access Type Modifiers



Step 2 Click the **Filter** button after entering the search criteria to display the filtered results.

The **Clean Access Server** column in the list shows the scope of the policy. If the policy was configured locally in the CAS management pages, this field displays the IP address of the originating Clean Access Server. If the policy was configured globally for all Clean Access Servers in the **Device Management > Filters** module of the admin console, the field displays GLOBAL.

The filter list can be sorted by column by clicking on the column heading label (MAC Address, IP Address, Clean Access Server, Description, Access Type, or Priority).

See Global and Local Administration Settings, page 2-8 and the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for more information.

Clicking **Reset** negates any of the optional search criteria from the filter dropdown menu and resets the list to display all entries (default).

Clicking **Delete Selected** removes the devices selected in the check column to the far left of the page. (You can select one or more device entries to remove from the display.)

Clicking **Delete All Filtered** removes the devices that remain in the list after you have used the **Filter** tool to display a subset of all devices. (You can use this function to remove up to 100 devices at a time.)

Import/Export Device Filter Policies

You can use the **Export** button to save CSV files containing device data to your local hard drive to search, view, and manipulate whenever needed for troubleshooting or statistical analysis purposes.

Note Due to limits native to the Microsoft Excel application, you can only export up to 65534 MAC address entries using this function.

You can also use the **Browse** and **Import** buttons to locate and load a compilation of device entries from a previously saved CSV file.

Order Device Filter Wildcard/Range Policies

The **Order** page is for **wildcard/range** device filters **only**. The **Order** page is used to change the priority of wildcard/range device filters.

For example:

- If the **Order** page is configured with filters as follows:
  1. 00:14:6A:* — Access Type: DENY
  2. 00:14:6A:6B:* — Access Type: IGNORE

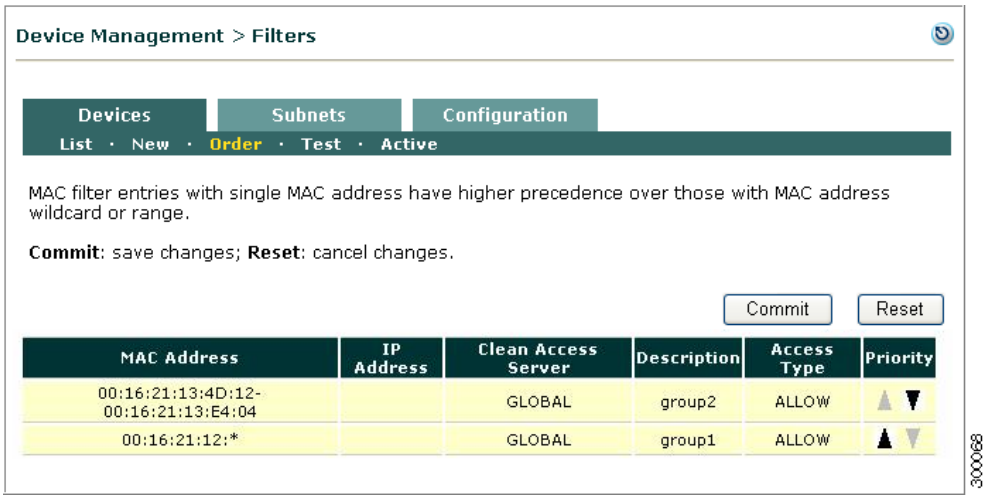
  A device with MAC address 00:14:6A:6B:60:60 will be denied.
- If the **Order** page is configured as follows:
  1. 00:14:6A:6B:* — Access Type: IGNORE
  2. 00:14:6A:* — Access Type: DENY

  A device with MAC address 00:14:6A:6B:60:60 will have access type IGNORE.

However, if a device filter exists for the exact MAC address 00:14:6A:6B:60:60, the rules of that filter apply instead, and any existing wildcard/range filters are not used.

1. Go to **Device Management > Filters > Devices > Order**.

Figure 2-9 Order



2. Click the arrows in the **Priority** column to move the priority of the wildcard/range filter up or down.
3. Click **Commit** to apply the changes. (Click **Reset** to cancel the changes.)

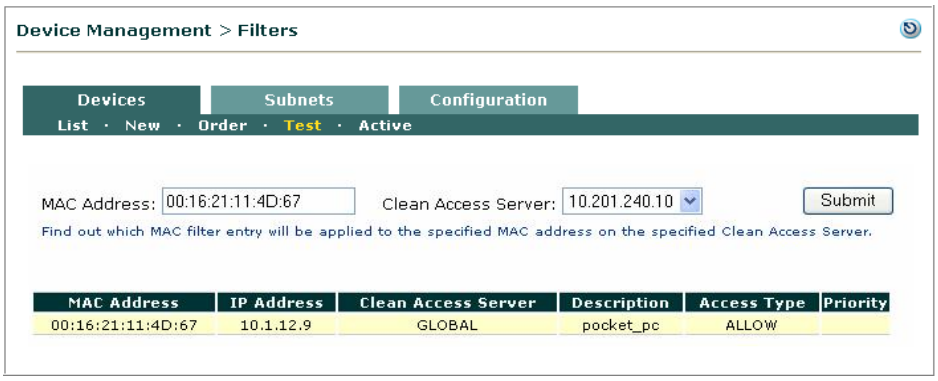
Note For more information on In-Band vs. Out-of-Band client machine behavior based on specified Device Filter type, see In-Band and Out-of-Band Device Filter Behavior Comparison, page 2-16.

Test Device Filter Policies

The **Test** page control allows administrators to determine which device filter and access type will be applied to the specified MAC address for a particular Clean Access Server.

1. Go to **Device Management > Filters > Devices > Test**.
2. Type the MAC address of the device in the **MAC Address** field.
3. Choose CAS to test against from the **Clean Access Server** dropdown menu.
4. Click **Submit**. The **Access Type** specified for the corresponding device filter appears in the list below.

Figure 2-10 Test



View Active Layer 2 Device Filter Policies

The Active Layer 2 In-Band Device Filters list displays all clients currently connected to the CAS, sending packets, and with their MAC addresses in a device filter. This list is especially useful in cases where users are configured to bypass authentication (via device filters) and/or posture assessment (such as when no requirements are enforced). Though by definition these users will not appear in the Online Users list or Certified Devices List, they can still be tracked on the In-Band network through the Active Layer 2 Device Filters List.

Note For more information on In-Band vs. Out-of-Band client machine behavior based on specified Device Filter type, see In-Band and Out-of-Band Device Filter Behavior Comparison, page 2-16.

To view active Layer 2 devices in filter policies across all Clean Access Servers:

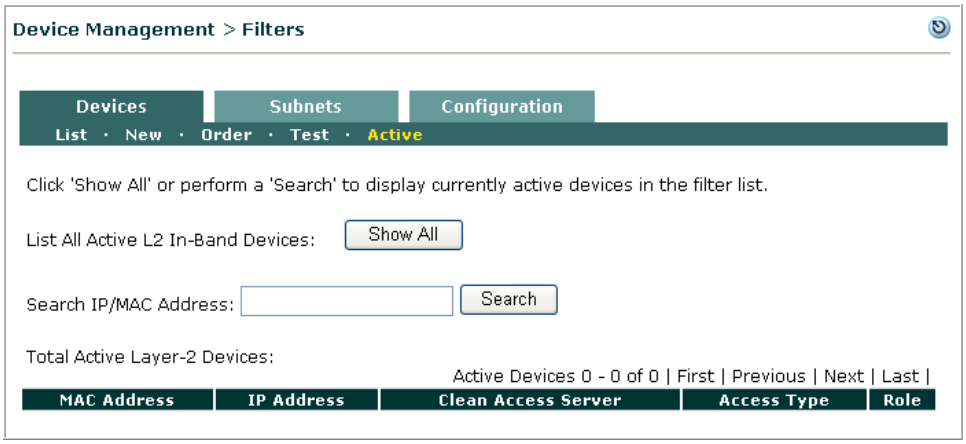
Step 1 Go to **Device Management > Filters > Devices > Active**.

Step 2 Click the **Show All** button first to populate the **Active** page with the information from all clients currently connected to the CAS, sending packets, and with their MAC addresses in a device filter.

You can also perform a **Search** on a client IP or MAC address to populate the page with the result. By default, the **Search** parameter performed is equivalent to "contains" for the value entered in the **Search IP/MAC Address** field.

Note For performance considerations, the **Active** page only displays the most current device information when you refresh the page by clicking **Show All** or **Search**.

Figure 2-11 Active


Device Management > Filters
Devices
Subnets
Configuration
List · New · Order · Test · Active
Click 'Show All' or perform a 'Search' to display currently active devices in the filter list.
List All Active L2 In-Band Devices:
Show All
Search IP/MAC Address:
Search
Total Active Layer-2 Devices:
Active Devices 0 - 0 of 0 | First | Previous | Next | Last |
MAC Address
IP Address
Clean Access Server
Access Type
Role
300065

Note To view active devices for an individual CAS, go **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Devices > Active**.

Edit Device Filter Policies

Step 1 Click the **Edit** icon next to device filter policy in the filter list. The **Edit** page appears similar to Figure 2-7.

Step 2 You can edit the IP Address, Description, Access Type, and Role used. Click **Save** to apply the changes.

Note Note that the MAC address is not an editable property of the filter policy. To modify a MAC address, create a new filter policy and delete the existing policy (as described below).

Delete Device Filter Policies

There are three ways to delete a device access policy or policies:

- Select the checkbox next to it in the **List** tab and click the **Delete Selected** button. Up to 25 device access policies per page can be selected and deleted in this way.
- Use the **Delete All Filtered** button to remove devices that remain in the list after you have used the **Filter** tool to display a subset of all devices.
- Use the search criteria to select the desired device filter policies and click **Delete List**. This removes all devices filtered by the search criteria across the number of applicable pages. Devices can be selectively removed using any of the search criteria used to display devices. The "filtered devices indicator" shown in Figure 2-8 displays the total number of filtered devices that will be removed when **Delete List** is clicked.

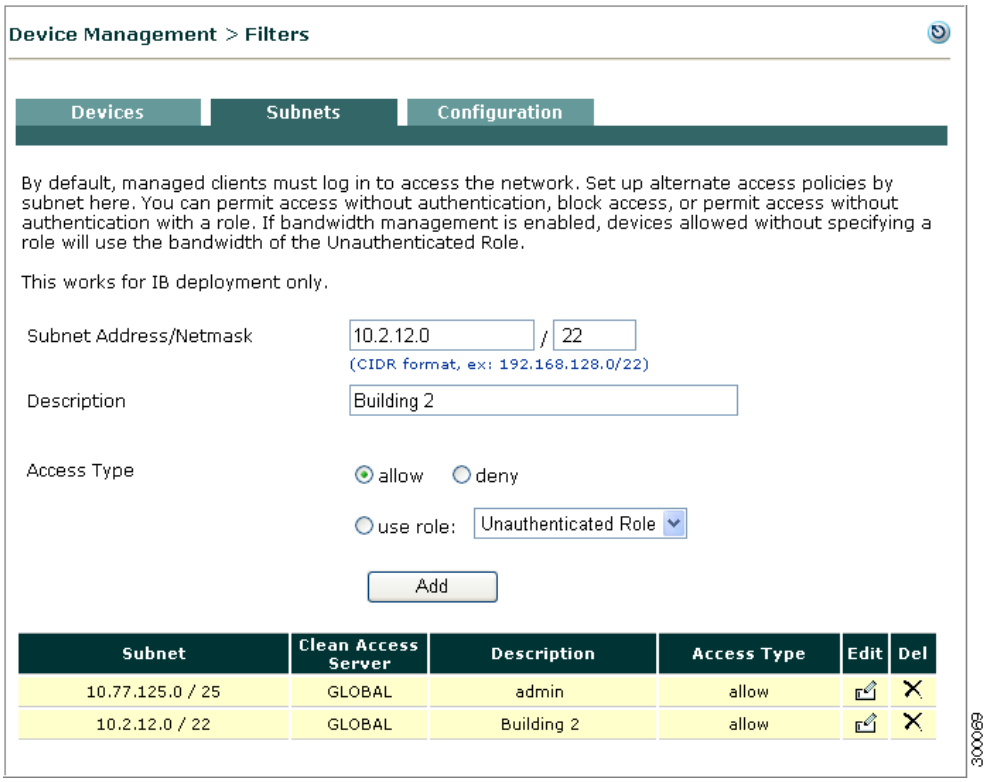
Configure Subnet Filters

The **Subnets** tab (Figure 2-12) allows you to specify authentication and access filter rules for an entire subnet. All devices accessing the network on the subnet are subject to the filter rule.

To set up subnet-based access controls:

Step 1 Go to **Device Management > Filters > Subnets**.

Figure 2-12 Subnet Filters



Step 2 In the **Subnet Address/Netmask** fields, enter the subnet address and subnet mask in CIDR format.

Step 3 Optionally, type a **Description** of the policy or device.

Step 4 Choose the network **Access Type** for the subnet:

- **allow** – Enables devices on the subnet to access the network without authentication.
- **deny** – Blocks devices on the subnet from accessing the network.
- **use role** – Allows access without authentication and applies a role to users accessing the network from the specified subnet. If you select this option, also select the role to apply to these devices. See Chapter 6, "User Management: Configuring User Roles and Local Users" for details on user roles.

Step 5 Click **Add** to save the policy.

The policy takes effect immediately and appears at the top of the filter policy list.

Note If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role. See Control Bandwidth Usage, page 8-13 for details.

After a subnet filter is added, you can remove it using the **Delete** icon or edit it by clicking the **Edit** icon. Note that the subnet address is not an editable property of the filter policy. To modify a subnet address, you need to create a new filter policy and delete the existing one.

The **Clean Access Server** column in the list of policies shows the scope of the policy. If the policy was configured as a local setting in a Clean Access Server, this field identifies the CAS by IP address. If the policy was configured globally in the Clean Access Manager, the field displays GLOBAL.

The filter list can be sorted by column by clicking on the column heading label (Subnet, Clean Access Server, Description, Access Type).

Integrating Cisco ISE Profiler

The Cisco Identity Services Engine (ISE) Profiler 1.0.4 can be integrated with Cisco NAC Appliance 4.9 and the ISE Profiler endpoints can be synchronized with the NAC Appliance.

For more details on Cisco ISE Profiler, refer to the following guides:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Note You can integrate only Cisco ISE Profiler, Release 1.0.4 and later with Cisco NAC Appliance, Release 4.9 and later. The earlier versions of ISE and NAC Appliance are not supported.

Limitations

- You can use either the NAC Profiler or the ISE Profiler at a time and you cannot use both the Profilers simultaneously.
- When you are upgrading from a previous version of NAC Appliance using NAC Profiler to release 4.9, all the endpoints along with Access Type policies added in the “Filters” are migrated to release 4.9. When you replace Nac Profiler with ISE Profiler, you need to configure the rules in NAC Manger for the Access Type policies in the endpoints.

Note The “NAC-Events” created in NAC Profiler are not available in ISE Profiler. They should be configured as “Rules” in CAM.

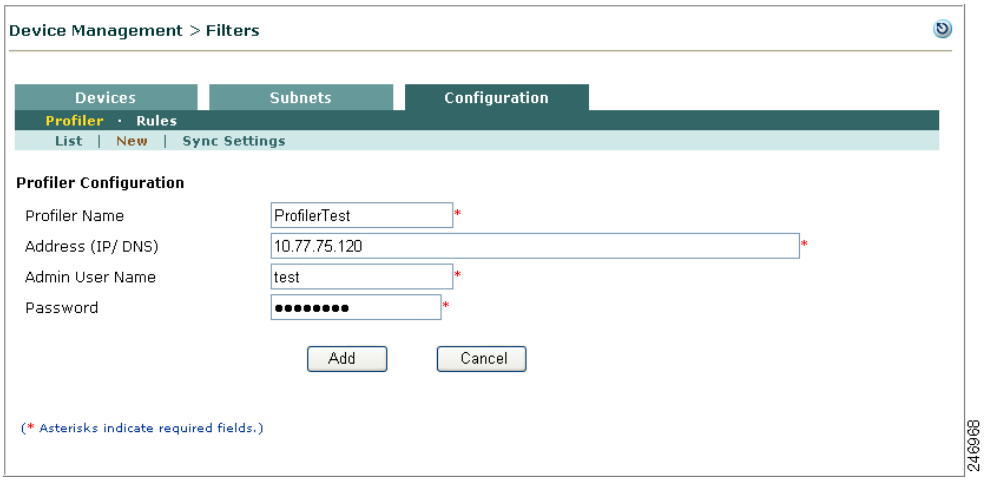
This section describes the following:

- Add Cisco ISE Profiler Details, page 2-30
- Display/Edit/Delete Cisco ISE Profiler Details, page 2-31
- Synchronize Endpoints from Cisco ISE Profiler, page 2-32
- Map Endpoint Policies, page 2-33
- Troubleshooting when Synchronizing the Cisco ISE, page 2-38

Add Cisco ISE Profiler Details

Step 1 In the CAM Web Console, navigate to **Device Management > Filters > Configuration > Profiler > New**.

Figure 2-13 Adding ISE Profiler Details



Step 2 Enter the Cisco ISE Profiler details as follows:

- **Profiler Name** – Enter any descriptive name for the Cisco ISE Profiler.
- **Address (IP/DNS)** – Enter the IP Address or the DNS Name of the Cisco ISE.
- **Admin User Name** – Enter the admin user name of Cisco ISE.
- **Password** – Enter the Password.

Step 3 Click **Add** to save the configuration details.

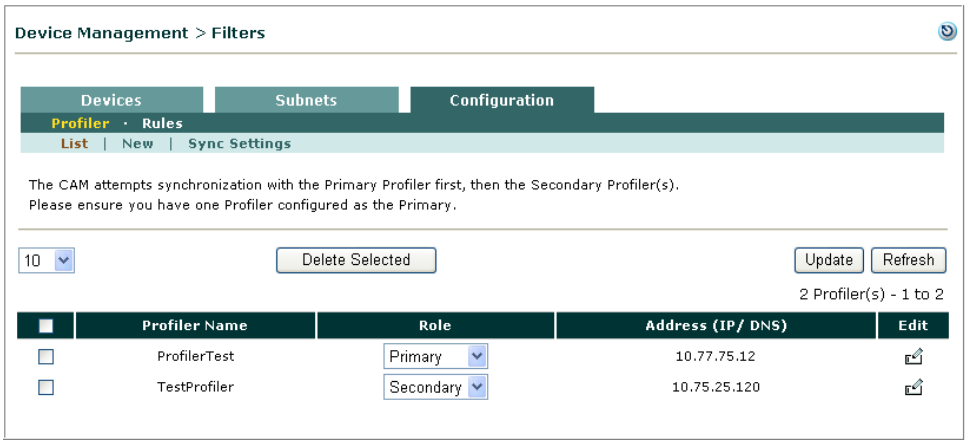
Note By default, the first ISE Profiler added to CAM is recognized as the "Primary" Profiler and the other ISE Profilers added are saved as "Secondary" Profilers. You can change this setting in **Device Management > Filters > Configuration > Profiler > List**. See Display/Edit/Delete Cisco ISE Profiler Details, page 2-31.

Display/Edit/Delete Cisco ISE Profiler Details

You can view the list of ISE Profilers added, edit the configuration details, or remove ISE Profiler using the **List** page.

Step 1 Navigate to **Device Management > Filters > Configuration > Profiler > List.**

Figure 2-14 List of ISE Profiler Details



Step 2 You can update the following:

- Choose the **Role** of the ISE Profiler as Primary or Secondary from the dropdown.
- Click the **Edit** icon next to the ISE Profiler Name to modify the details.
- Click the checkbox preceding the ISE Profiler Name and click **Delete Selected** to remove a Profiler.

Step 3 Click **Update** to save the changes. Click **Refresh** to revert to the previous settings.

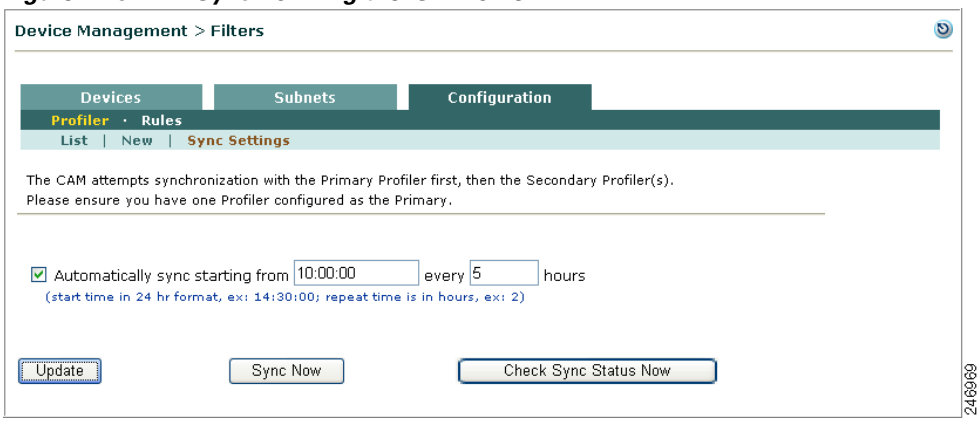
Note You can designate only one Profiler as "Primary" at a time. Other profilers are designated as secondary. While synchronizing with ISE, if NAC fails to connect to the Primary, it tries to connect to the available Secondary Profiler in a sequence.

Synchronize Endpoints from Cisco ISE Profiler

After configuring the ISE Profiler details in the CAM Web Console, CAM can synchronize all the endpoints from ISE Profiler either automatically or manually by using the **Sync Settings**.

Step 1 Navigate to **Device Management > Filters > Configuration > Profiler > Sync Settings**.

Figure 2-15 Synchronizing the ISE Profiler


Device Management > Filters
Devices
Subnets
Configuration
Profiler · Rules
List | New | Sync Settings
The CAM attempts synchronization with the Primary Profiler first, then the Secondary Profiler(s).
Please ensure you have one Profiler configured as the Primary.
Automatically sync starting from 10:00:00 every 5 hours
(start time in 24 hr format, ex: 14:30:00; repeat time is in hours, ex: 2)
Update
Sync Now
Check Sync Status Now
246969

Step 2 **Automatically sync starting from [] every [] hours** – Enter the time at which the synchronization should start in 24-hour format and enter the number of hours at which the synchronization should be repeated.

Step 3 Click **Update** save the settings.

Step 4 Click **Sync Now** to start the synchronization manually.

Note When synchronizing automatically or manually, CAM deletes all the existing end-points in the CAM Filter List and pulls all the end-points from ISE Profiler by applying the Rules (Matching Profiles) configured in CAM.

You can click **Check Sync Status Now** to check the current synchronization status. This option displays the following details: the last synchronized date and time, number of endpoints synchronized, and time taken for synchronization.

Note While synchronizing, NAC searches for the Primary Profiler. If it is not reachable, then it searches for the Secondary Profilers, one by one in the List. You should have already selected one of the Profilers in the **List** as "Primary."

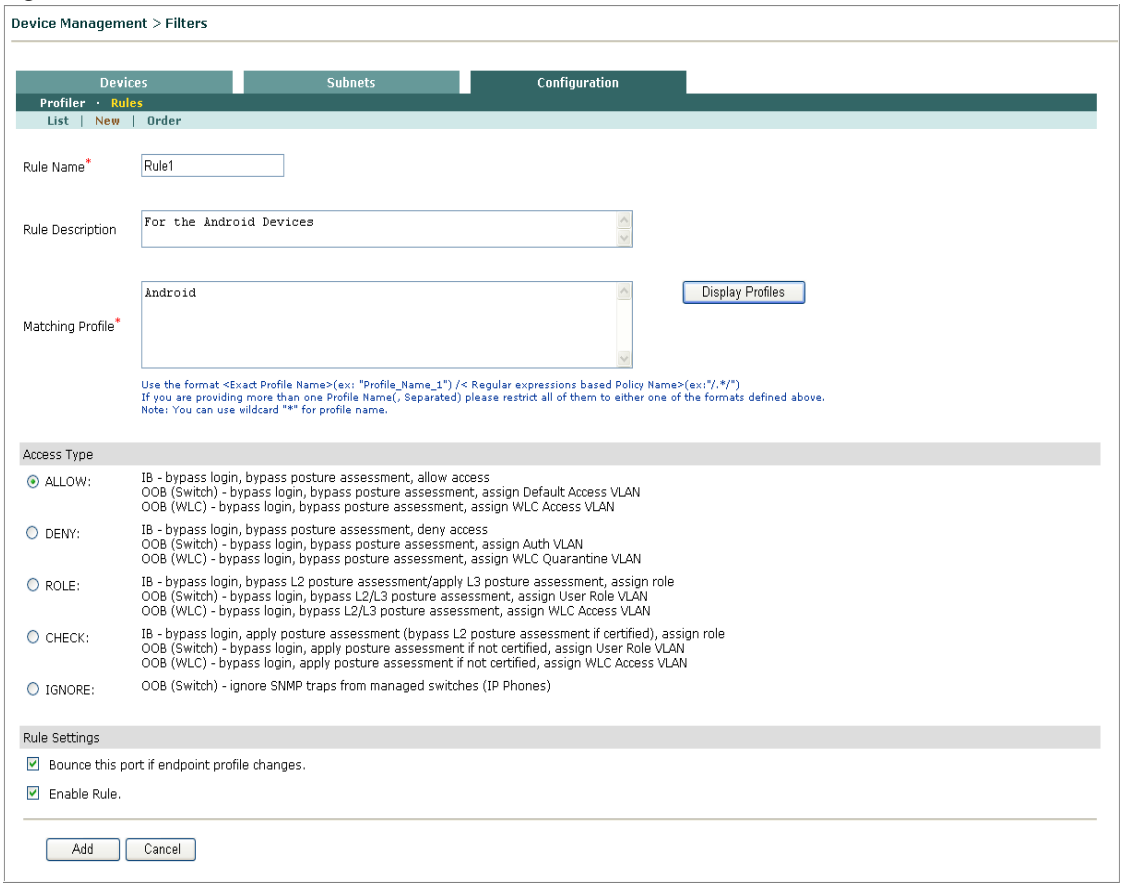
Map Endpoint Policies

You can create rules with the endpoint profiles that are already existing in the Cisco ISE Profiler and map them to the CAM.

Create New Rule

Step 1 Go to **Device Management > Filters > Configuration > Rules > New**.

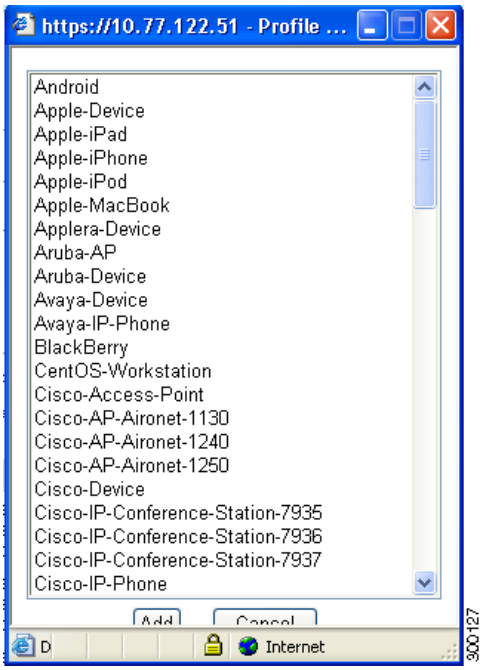
Figure 2-16 New Rule


Device Management > Filters
Devices
Subnets
Configuration
Profiler · Rules
List | New | Order
Rule Name*
Rule1
Rule Description
For the Android Devices
Matching Profile*
Android
Display Profiles
Use the format <Exact Profile Name>(ex: "Profile_Name_1") /< Regular expressions based Policy Name>(ex:"/.*/")
If you are providing more than one Profile Name(, Separated) please restrict all of them to either one of the formats defined above.
Note: You can use wildcard "*" for profile name.
Access Type
ALLOW:
IB - bypass login, bypass posture assessment, allow access
OOB (Switch) - bypass login, bypass posture assessment, assign Default Access VLAN
OOB (WLC) - bypass login, bypass posture assessment, assign WLC Access VLAN
DENY:
IB - bypass login, bypass posture assessment, deny access
OOB (Switch) - bypass login, bypass posture assessment, assign Auth VLAN
OOB (WLC) - bypass login, bypass posture assessment, assign WLC Quarantine VLAN
ROLE:
IB - bypass login, bypass L2 posture assessment/apply L3 posture assessment, assign role
OOB (Switch) - bypass login, bypass L2/L3 posture assessment, assign User Role VLAN
OOB (WLC) - bypass login, bypass L2/L3 posture assessment, assign WLC Access VLAN
CHECK:
IB - bypass login, apply posture assessment (bypass L2 posture assessment if certified), assign role
OOB (Switch) - bypass login, apply posture assessment if not certified, assign User Role VLAN
OOB (WLC) - bypass login, apply posture assessment if not certified, assign WLC Access VLAN
IGNORE:
OOB (Switch) - ignore SNMP traps from managed switches (IP Phones)
Rule Settings
Bounce this port if endpoint profile changes.
Enable Rule.
Add
Cancel
246971

Step 2 In the **New** Rule form, enter the following:

- **Rule Name** – Enter a name for the new Rule.
- **Rule Description** – Enter a description.
- **Matching Profile** – Enter Endpoint Profile names in the text box as follows:
  - Specify an exact Profile name. You can click **Display Profiles** and select a Profile from the popup list. The existing endpoint Profile names in Cisco ISE Profiler are displayed in this list as shown in Figure 2-17.
  - Use a wildcard "*" to specify multiple Profile names.
  - Separate multiple Profile names with a return.

Figure 2-17 Display Profiles



Step 3 Choose the policy for the Profile from the **Access Type** choices:

- **ALLOW**
  IB - bypass login, bypass posture assessment, allow access
  OOB (Switch) - bypass login, bypass posture assessment, assign Default Access VLAN
  OOB (WLC) - bypass login, bypass posture assessment, assign WLC Access VLAN
- **DENY**
  IB - bypass login, bypass posture assessment, deny access
  OOB (Switch) - bypass login, bypass posture assessment, assign Auth VLAN
  OOB (WLC) - bypass login, bypass posture assessment, assign WLC Quarantine VLAN
- **ROLE**
  IB - bypass login, bypass L2 posture assessment/apply L3 posture assessment, assign role
  OOB (Switch) - bypass login, bypass L2/L3 posture assessment, assign User Role VLAN
  OOB (WLC) - bypass login, bypass L2/L3 posture assessment, assign WLC Access VLAN. See Chapter 6, "User Management: Configuring User Roles and Local Users" for details.

- **CHECK**
  IB - bypass login, apply posture assessment (bypass L2 posture assessment if certified), assign role
  OOB (Switch) - bypass login, apply posture assessment if not certified, assign User Role VLAN
  OOB (WLC) - bypass login, apply posture assessment if not certified, assign WLC Access VLAN
- **IGNORE**
  OOB (Switch) - ignore SNMP traps from managed switches (IP Phones)

Step 4 **Bounce this port if endpoint profile changes** – Check this option if you want to bounce the port when there is a change in an endpoint profile. This is applicable only to OOB deployments.

Step 5 **Enable Rule** – Check this option to enable the rule.

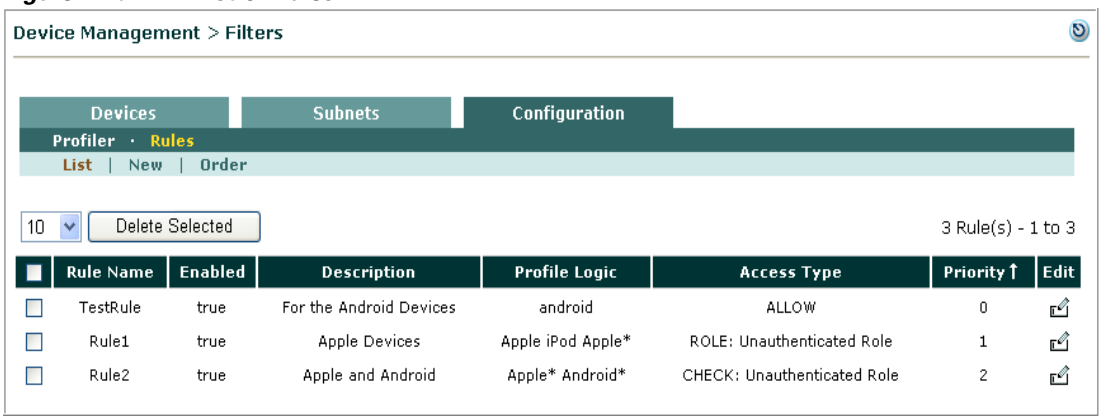
Step 6 Click **Add** to save the Rule.

CAM pulls all the endpoints available in the ISE Profiler and applies the Access Type selected in the matching rules. If an endpoint is not matching with any of the rules, the Access Type "DENY" is applied to it.

View Rules

Click the **List** tab under **Rules** to view the existing rules as shown in Figure 2-18.

Figure 2-18 List of Rules



The **List** tab displays the Rule Names, whether the rules are enabled or not, description, profiles, access types, and priority. You can edit or delete a rule as described in the following sections.

Edit Rules

Step 1 Go to **Device Management > Filters > Configuration > Rules > List.**

Step 2 Click the **Edit** icon corresponding to the Rule Name in the Rules list. An **Edit** window similar to Figure 2-16 is displayed.

Step 3 You can edit the Rule Name, Rule Description, Matching Profile, Access Type and the User Role used.

Step 4 Click **Update** to apply the changes.

Delete Rules

To delete a rule, in the **Device Management > Filters > Configuration > Rules > List** tab, click the checkbox preceding the Rule Name in the List and click the **Delete Selected** button.

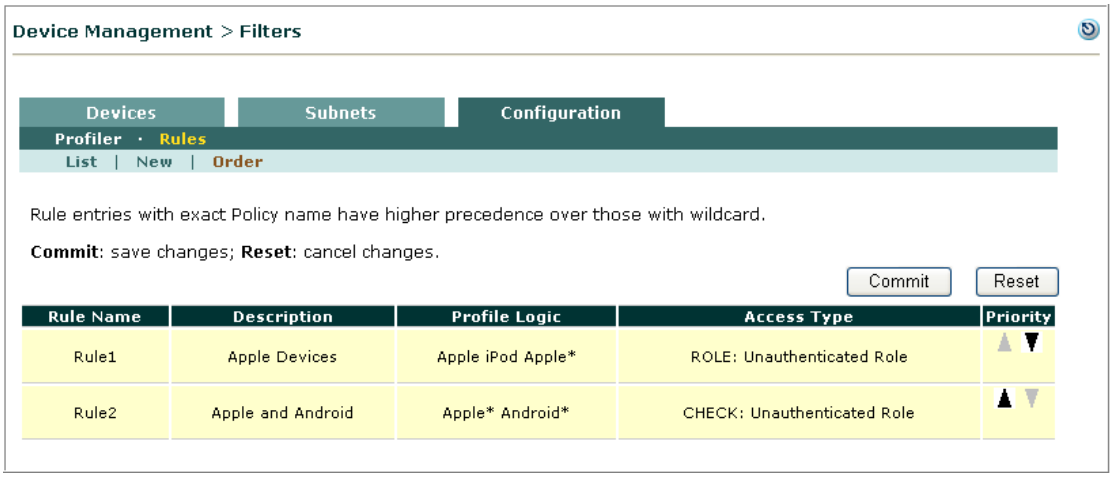
The selected rules are removed from the list.

Order Rules

The **Order** page can be used to change the priority of the Rules. Rule names with exact Profile names have higher priority than the Profile names which use wildcards. You can change the priority only for profile names that contain wildcards.

Step 1 Go to **Device Management > Filters > Configuration > Rules > Order**.

Figure 2-19 Order Rules



Step 2 Click the arrows in the **Priority** column to move the priority of the Rules up or down.

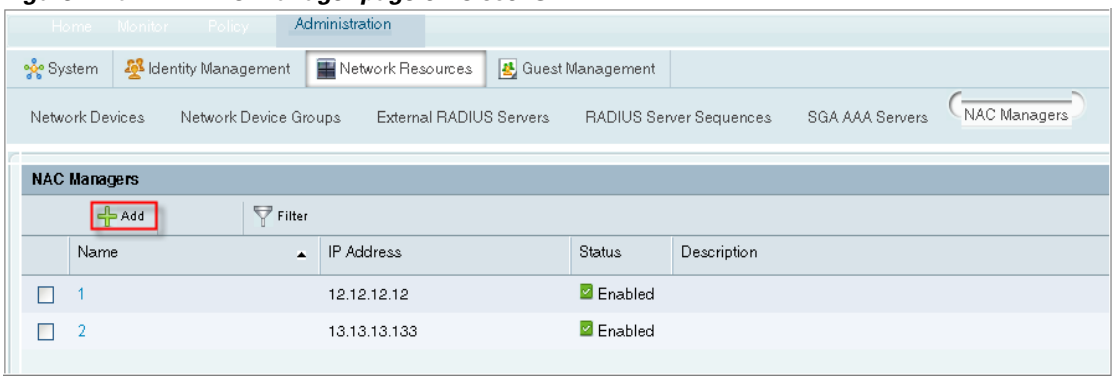
Step 3 Click **Commit** to apply the changes. (Click **Reset** to cancel the changes.)

Configure NAC Manager in ISE Profiler

You need to configure the NAC Manager (CAM) details into the Cisco ISE Profiler in order for the CAM to obtain endpoint profile information from the ISE Profiler.

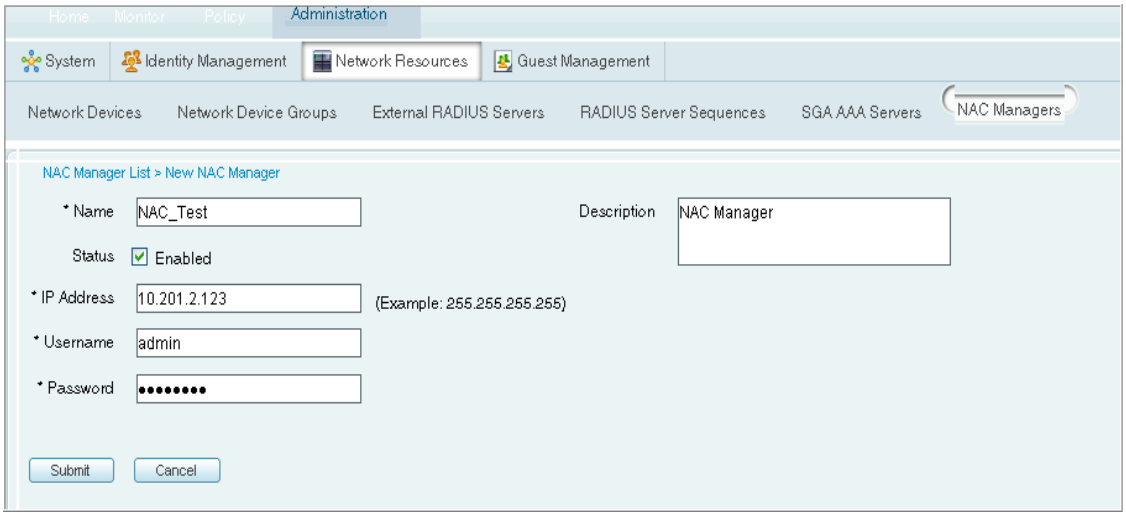
Step 1 In the Cisco ISE web console, go to **Administration > Network Resources > NAC Managers**. The NAC Managers page appears as shown in Figure 2-20.

Figure 2-20 NAC Manager page on Cisco ISE



Step 2 In the NAC Managers page, click **Add**. The New NAC Manager page appears as shown in Figure 2-21.

Figure 2-21 Adding NAC Manager to ISE Profiler



Step 3 Enter the NAC Manager (CAM) details as follows:

- **Name** – Enter any descriptive name for the CAM.
- **Description** – Optionally, enter a description for the CAM.
- **Status** – Click the check box to enable communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
- **IP Address** – Enter the IP Address of the CAM. (For example, 255.255.255.255).

Note For High-Availability configurations, use the Service IP of the CAM. This allows failover support of CAMs in High-Availability configuration.

Note Once saved, the IP Address of the CAM cannot be edited.

- **Username** – Enter the name of the CAM web console admin user.
- **Password** – Enter the password for the CAM web console admin user.

Step 4 Click **Submit**.

For further details on the Cisco ISE Profiler, refer to the *Cisco Identity Services Engine User Guide* on Cisco.com at:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Troubleshooting when Synchronizing the Cisco ISE

While synchronizing CAM with endpoints from Cisco ISE, the CAM tries to pull the details from Cisco ISE. If you have issues while pulling the data, check the following:

- Go to **Device Management > Filters > Configuration > Profiles > Configure > List** and check the ISE Profiler configuration.
  - Check the IP Address, Admin User Name, and Password.
  - Check whether the CAM is able to reach ISE Profiler.
- Go to **Device Management > Filters > Configuration> Rules** and check the rules configured.
  - Check the priority of rules set for regular expressions.
  - If the end-point got denied, check whether proper rule has been configured and enabled.
- Go to **Device Management > Filters > Configuration > Profiler > Sync Settings** page and click **Check Sync Status Now**. The log messages that are displayed provide more information about the synchronization.

While synchronizing Cisco ISE with CAM, the Cisco ISE tries to push the details to CAM. If you have issues while pushing the data, check the following:

- In the Cisco ISE web console, go to **Administration > Network Resources > NAC Managers**.
- In the **NAC Managers** page, check the details of the CAM and the credentials.

Example Scenarios

Note The following are sample messages that may be displayed during various scenarios of synchronization.

Primary ISE connection failed, Secondary ISE is connected

```
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Trying to connect to the URL:
https://9.9.9.11/ise/ProfilerConfig/EndPointPartial
2011-08-26 15:13:59.912 +0530   DefaultQuartzScheduler_Worker-1 ERROR
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - IOException:
java.net.NoRouteToHostException: No route to host
```

The above message is displayed when connection to Primary ISE has failed. This may happen when there is an issue with the connectivity or when the credentials are not correct.

```
2011-08-26 15:13:59.949 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Connected to the URL :
https://9.9.10.10/ise/ProfilerConfig/EndPointPartial
```

The above is displayed when CAM is trying to connect to secondary ISE.

```
2011-08-26 15:14:01.014 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Opening url inputstream - took 0
hour(s) 0 minute(s) 1 second(s) 101 milli(s)
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Finished executing the jobTook -
took 0 hour(s) 0 minute(s) 4 second(s) 44 milli(s)
2011-08-26 15:14:03.952 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Sync job execution completed.
2011-08-26 15:14:03.952 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.perfigo.wlan.web.admin.SmartManagerConf        - SMC - STORE: UPDATE
smartmanager_conf SET prop_value='Synched with profiler 9.9.10.10 at 08/26/2011
15:13:59 [format: MM/DD/YYYY HH:mm:ss]# Number of endpoints synched - 149# Time taken
- 0 hour(s) 0 minute(s) 4 second(s) 44 milli(s)#' WHERE prop_name='ProfilerSyncStatus'
```

The above means the connection is successful.

Cisco ISE is not reachable

```
2011-08-29 14:21:02.767 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Executing a full sync job :
1314607862767
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - returning endpoints processed
2011-08-29 14:21:05.768 +0530   DefaultQuartzScheduler_Worker-1 ERROR
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - IOException:
java.net.NoRouteToHostException: No route to host
```

The above messages are displayed when CAM is not able to ping Cisco ISE. You should check the connectivity and the configuration.

```
2011-08-29 14:21:05.769 +0530   DefaultQuartzScheduler_Worker-1 ERROR
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - No route to host
2011-08-29 14:21:05.771 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.perfigo.wlan.web.admin.SmartManagerConf        - SMC - STORE: UPDATE
smartmanager_conf SET prop_value='Sync with profiler failed at 08/29/2011 14:21:02#
Reason -  Unable to obtain information from the configured profiler(s).
1) Please check the connectivity and configuration.
2) Check logs for more information#' WHERE prop_name='ProfilerSyncStatus'
```

CAM is able to reach Cisco ISE, but the credentials are invalid

```
2011-08-29 14:30:22.930 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Executing a full sync job :
1314608422930
2011-08-29 14:30:22.930 +0530   TP-Processor23 INFO
com.perfigo.wlan.web.admin.EventLog                - Profiler: Successfully scheduled
sync job of type:SYNC_NOW
2011-08-29 14:30:22.930 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - Trying to connect to the URL:
https://9.9.10.10/ise/ProfilerConfig/EndPointPartial
2011-08-29 14:30:22.941 +0530   TP-Processor23 INFO
com.cisco.nac.core.nacprofiler.SyncJobScheduler    - Successfully scheduled sync job
of type:SYNC_NOW
2011-08-29 14:30:22.969 +0530   DefaultQuartzScheduler_Worker-1 ERROR
com.cisco.nac.core.nacprofiler.job.FullSyncJob     - IOException: java.io.IOException:
Server returned HTTP response code: 401 for URL:
https://9.9.10.10/ise/ProfilerConfig/EndPointPartial
```

The above messages are displayed when Cisco ISE is reachable, but the credentials are not correct.

```
2011-08-29 14:30:22.971 +0530   DefaultQuartzScheduler_Worker-1 INFO
com.perfigo.wlan.web.admin.SmartManagerConf        - SMC - STORE: UPDATE
smartmanager_conf SET prop_value='Sync with profiler failed at 08/29/2011 14:30:22#
Reason -  Unable to obtain information from the configured profiler(s).
1) Please check the connectivity and configuration.
2) Check logs for more information#' WHERE prop_name='ProfilerSyncStatus'
```

You can also check the CAM log files by using the following commands:

```
/perfigo/control/tomcat/logs/nac_manager.log
/perfigo/control/tomcat/logs/catalina.out
```



Switch Management: Configuring Out-of-Band Deployment

This chapter describes how to configure Cisco NAC Appliance for Out-of-Band (OOB) deployment. Topics include:

- Overview, page 3-1
- Deployment Modes, page 3-5
- Configure Your Network for Out-of-Band, page 3-13
- Configure Your Switches, page 3-14
- Configure OOB Switch Management on the CAM, page 3-25
- Configure Access to Authentication VLAN Change Detection, page 3-67
- Out-of-Band Users, page 3-68
- OOB Troubleshooting, page 3-71
- Troubleshooting SNMP, page 3-72

See *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for additional information on L3 OOB deployment.

Overview

In a traditional In-Band Cisco NAC Appliance deployment, all network traffic to or from clients goes through the Clean Access Server. For high throughput or highly routed environments, a Cisco NAC Appliance Out-of-Band (OOB) deployment allows client traffic to pass through the Cisco NAC Appliance network only in order to be authenticated and certified before being connected directly to the access network. This section discusses the following topics:

- In-Band Versus Out-of-Band, page 3-2
- Out-of-Band Requirements, page 3-2
- SNMP Control, page 3-4

In-Band Versus Out-of-Band

Table 3-1 summarizes different characteristics of each type of deployment.

Table 3-1 In-Band vs. Out-of-Band Deployment

In-Band Deployment Characteristics	Out-of-Band Deployment Characteristics
The Clean Access Server (CAS) is always inline with user traffic (both before and following authentication, posture assessment and remediation). Enforcement is achieved through being inline with traffic.	The Clean Access Server (CAS) is inline with user traffic only during the process of authentication, assessment and remediation. Following that, user traffic does not come to the CAS. Enforcement is achieved through the use of SNMP to control switches and VLAN assignments to ports.
The CAS can be used to securely control authenticated and unauthenticated user traffic by using traffic policies (based on port, protocol, subnet), bandwidth policies, and so on.	The CAS can control user traffic during the authentication, assessment and remediation phase, but cannot do so post-remediation since the traffic is Out-of-Band.
Does not provide switch port level control.	Provides port-level control by assigning ports to specific VLANs as necessary.
In-Band deployment is supported when deploying for wireless networks.	Wireless OOB requires a specific network topology and configuration. For more information, see Chapter 4, "Wireless LAN Controller Management: Configuring Wireless Out-of-Band Deployment."
Cisco NAC Appliance In-Band deployment with supported Cisco switches is compatible with 802.1x	Cisco does not recommend using 802.1x in an OOB deployment, as conflicts will likely exist between Cisco NAC Appliance OOB and 802.1x to set the VLAN on the switch interfaces/ports.

Out-of-Band Requirements

Out-of-band implementation of Cisco NAC Appliance requires the following to be in place:

- Controlled switches must be supported models (or service modules) that use at least the minimum supported version of IOS or CatOS (supporting MAC change notification/MAC move notification or linkup/linkdown SNMP traps).

  Supported switch models include:

  - Cisco Catalyst Express 500 Series
  - Cisco Catalyst 2900 XL
  - Cisco Catalyst 2940/2950/2950 LRE/2955/2960
  - Cisco Catalyst 3500 XL
  - Cisco Catalyst 3550/3560/3750/3850
  - Cisco Catalyst 4000/4500/4948
  - Cisco Catalyst 6000/6500

Note Cisco Catalyst 3850 switches are supported starting from Cisco NAC Appliance Release 4.9(4).

Supported 3750 service modules for Cisco 2800/3800 Integrated Services Routers (ISR) include:

- NME-16ES-1G
- NME-16ES-1G-P
- NME-X-23ES-1G
- NME-X-23ES-1G-P
- NME-XD-24ES-1S-P
- NME-XD-48ES-2S-P

Note The support for Cisco NAC Network Module for Integrated Services Routers (NME-NAC-K9) has been removed from Cisco NAC Appliance Release 4.9(4).

- Your Cisco NAC Appliance product license must enable OOB.

Note

- With IOS release 12.2.25(SEG) for CE500, MAC notification SNMP traps are supported on all Smartport roles (including DESKTOP and IPPHONE roles). After upgrading to 12.2.25(SEG), customers can configure MAC notification for CE500 under **OOB Management > Devices > List > Config [Switch IP] > Config > Advanced** on the CAM. For Cisco NAC Appliance 3.6.2, 3.6.3, 4.0.0, 4.0.1, 4.0.2, CE500 supports linkup/linkdown SNMP notifications by default and the "OTHER role" warning message can be ignored when changing to MAC notification traps. In later Cisco NAC Appliance releases, this warning message is removed and the default control method for CE500 is MAC notification traps.
- If running an IOS version earlier than 12.2(25) SEG, the CE500 switch ports must be assigned to the OTHER role (not Desktop or IP phone) on the switch's Smartports configuration; otherwise, MAC notification is not sent.

Note Cisco NAC Appliance OOB supports Cisco Catalyst 3750 StackWise technology. With stacks, when MAC notification is used and there are more than 252 ports on the stack, MAC notification cannot be set/unset for the 252nd port using the CAM. There are two workarounds: 1) Use linkup/linkdown SNMP notifications only. 2) If using MAC notification, do not use the 252nd port and ignore the error; other ports will work fine.

Clusters are not supported.

Note For the most current details on switch model/IOS/CatOS version support, refer to *Switch Support for Cisco NAC Appliance*.

SNMP Control

With Out-of-Band deployment, you can add switches to the Clean Access Manager's domain and control particular switch ports using the Simple Network Management Protocol (SNMP). SNMP is an application layer protocol used by network management tools to exchange management information between network devices. Cisco NAC Appliance supports the following SNMP versions:

CAM to OOB Switch	OOB Switch to CAM (Traps)
Read: • SNMP V1 • SNMP V2c (V2 with community string) • SNMP V3 **Write:** • SNMP V1 • SNMP V2c • SNMP V3	• SNMP V1 • SNMP V2c • SNMP V3

You first need to configure the switch to send and receive SNMP traffic to/from the Clean Access Manager, then configure matching settings on the Clean Access Manager to send and receive traffic to/from the switch. This will enable the Clean Access Manager to get VLAN and port information from the switch and set VLANs for managed switch ports.

Cisco NAC Appliance also provides support for SHA-1 and 3DES encryption, which is required when configuring SNMP management on a CAM operating in a FIPS 140-2 compliant network.

Network Recovery for "Off Line" Out-of-Band Switches

Cisco NAC Appliance features configurable SNMP polling behavior for Out-of-Band managed switches to ensure that the CAM is able to communicate with switches experiencing network issues when they return to normal operation. Without this function, Cisco NAC Appliance might lose communication with managed switches altogether and remain undetected for some time, requiring the Cisco NAC Appliance administrator to manually step in and clear up the switch behavior and re-establish CAM-to-switch communication.

You can configure this feature using the following settings in the **smartmanager_conf** table of the CAM CLI:

- **OobSnmpErrorLimit**—This is maximum number of consecutive SNMP timeout failures. If the number of consecutive failures reaches this value, the switch is disabled. If the administrator specifies the limit so that it is equal to or is less than 0, this feature is disabled. The default value is 10.
- **OobSnmpRecoverInterval**—This is the internal time period (in minutes) that the recovery process waits to check disabled switches to see if they have come back online. The default value is 10.

Deployment Modes

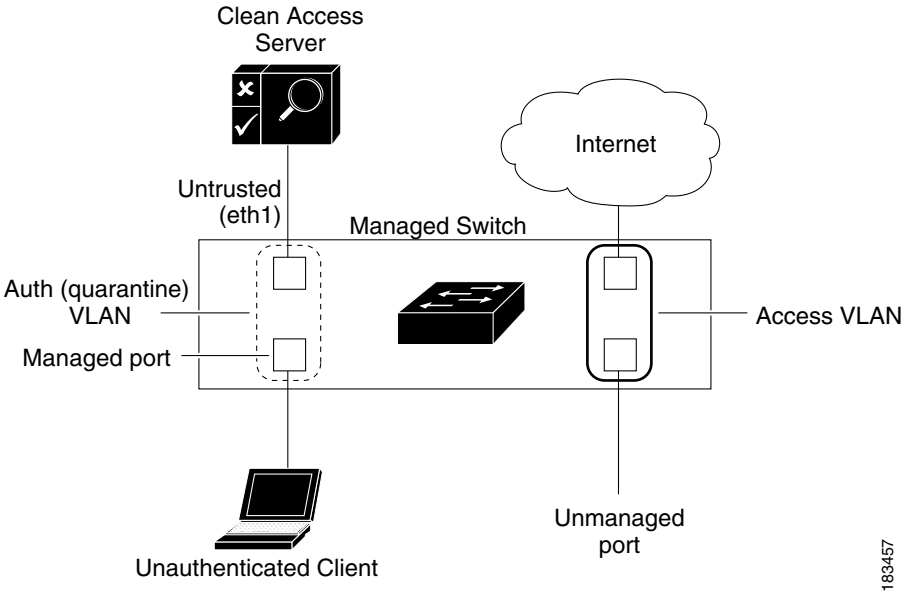
This section describes Out-of-Band deployment for Virtual Gateway and Real-IP. For all gateway modes, to incorporate Cisco NAC Appliance Out-of-Band in your network, you must add an Authentication VLAN to your network and trunk all Auth VLANs to the untrusted interface of the Clean Access Server.

- Basic Connection, page 3-5
- Out-of-Band Virtual Gateway Deployment, page 3-6
- Out-of-Band Real-IP Gateway Deployment, page 3-10
- L3 Out-of-Band Deployment, page 3-13

Basic Connection

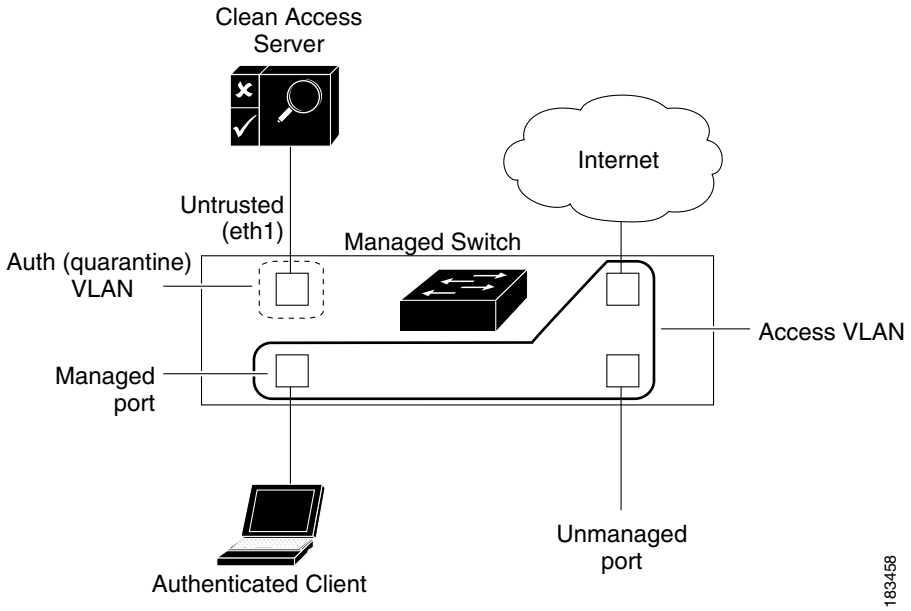
The following diagrams show basic "before" and "after" VLAN settings for a client attached to an Out-of-Band deployment. Figure 3-1 illustrates the In-Band client and Figure 3-2 illustrates the client when Out-of-Band.

Figure 3-1 Before — Client is In-Band for Authentication/Certification



When an unauthenticated client first connects to a managed port on a managed switch (Figure 3-1), the CAM instructs the switch to change the client port from the authentication (quarantine) VLAN specified in the Port Profile for the port. The switch then sends all traffic from the Auth VLAN client to the untrusted interface of the Clean Access Server (CAS). The client authenticates through the CAS, and/or goes through Nessus Scanning/posture assessment as configured for the role or device. Because the client is on the authentication VLAN, all the client's traffic must go through the CAS and the client is considered to be In-Band.

Figure 3-2 After — Client is Out-of-Band After Being Certified



Once the client is authenticated and certified (i.e. on the Certified Devices List), the CAM instructs the switch to change the VLAN of the client port to the Access VLAN specified in the Port Profile of the port (Figure 3-2). Once the client is on the Access VLAN, the switch no longer directs the client's traffic to the untrusted interface of the CAS. At this point the client is on the trusted network and is considered to be Out-of-Band.

In the event the user reboots the client machine, unplugs it from the network, or the switch port goes down, this triggers the switch to send a linkdown trap to the CAM. Thereafter, the client port behavior depends on the Port profile settings for the specific port (see Add Port Profile, page 3-34 for details).

If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to "kick" the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see Configure Access to Authentication VLAN Change Detection, page 3-67. (In earlier releases, the client machine would only learn of the switch after the DHCP lease for the client IP address had run out and could not reconnect.)

Note You can configure the Initial VLAN of the port to be the Access VLAN. See Add Port Profile, page 3-34 for details.

Out-of-Band Virtual Gateway Deployment

An Out-of-Band Virtual Gateway deployment provides the following benefits:

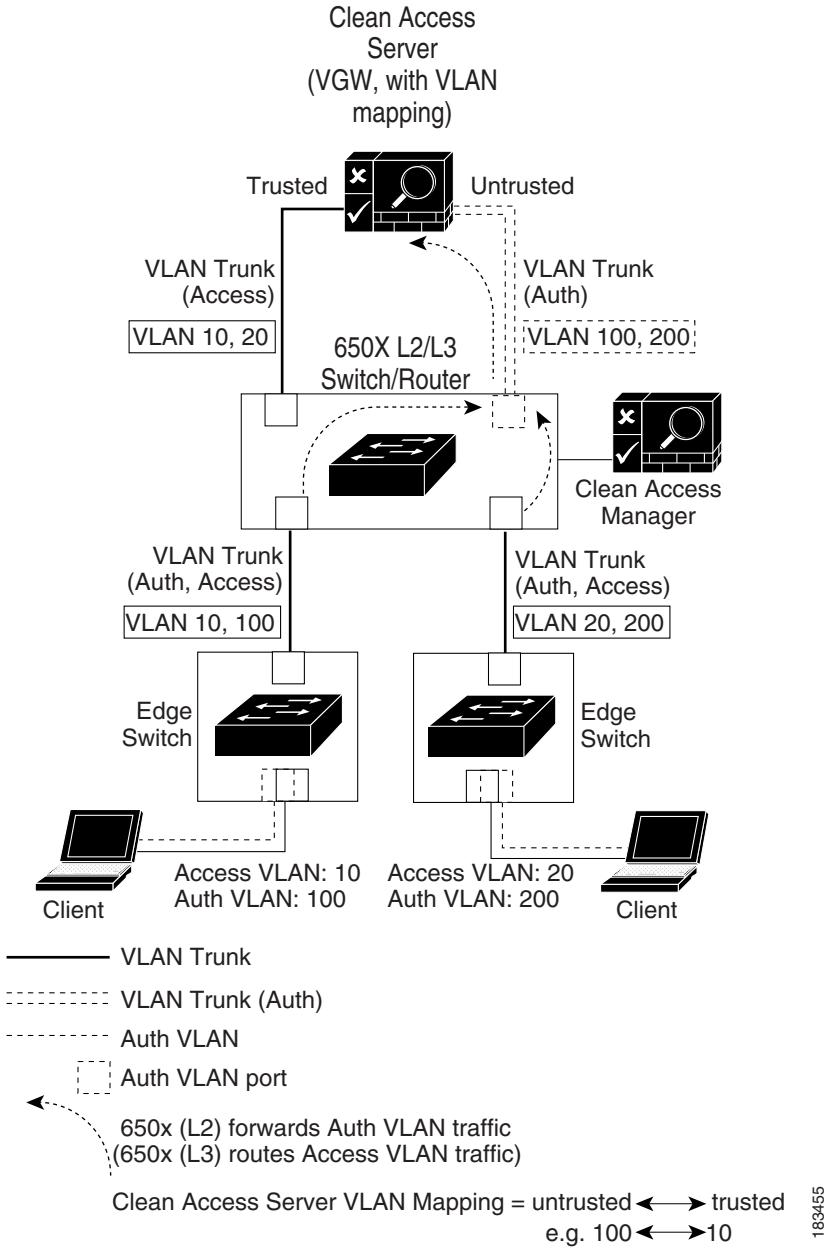
- The client never needs to change its IP address from the time it is acquired to the time the client gains actual network access on the Access VLAN.
- For L2 users, static routes are not required.

In Out-of-Band Virtual Gateway mode, the Clean Access Server uses the VLAN mapping feature to retag the unauthenticated client's allowed traffic (such as DNS or DHCP requests) from the Authentication VLAN to the Access VLAN and vice versa. In this way, no new client IP address is needed when the client is eventually switched to the Access VLAN, because the DHCP-acquired IP address is already paired with the Access VLAN ID.

Note In an environment where there is an 802.1q trunk to the CAS, the CAS will bridge two VLANs together. This "retagging" is the rewriting of the 802.1q Ethernet header with a new VLAN ID. This feature does not apply when there is only one Authentication VLAN and one Access VLAN, as no frames are tagged.

Figure 3-3 illustrates Out-of-Band Virtual Gateway mode using an L3 router/switch. The router/switch receives traffic from the Auth VLAN as Layer 2 traffic and forwards it to the untrusted side of the Clean Access Server. The Virtual Gateway Clean Access Server performs VLAN mapping for allowed traffic (DNS, DHCP) from the Auth VLAN (untrusted interface) to the Access VLAN (trusted interface) and vice versa. The router/switch receives traffic from the Access VLAN as Layer 3 traffic and routes it accordingly. Figure 3-3 illustrates the client authentication and access path for the OOB Virtual Gateway example described below. In this example, the Authentication VLAN is 100, and the Access VLAN is 10.

Figure 3-3 Out-of-Band VGW Mode: Catalyst 6500 Series Example



Flow for OOB VGW Mode

1. The unauthenticated user connects the client machine to the network through an access layer switch.
2. The switch sends MAC notification or linkup/linkdown SNMP traps for the client to the CAM. Because the client is not on the Certified Devices List/Online Users list yet, the CAM sends an SNMP SET trap to the switch instructing it to change the client port to the Auth VLAN specified in the Port Profile (100), and the CAM places the client on the Out-of-Band Wired Clients list (**OOB Management > Devices > Discovered Clients > Wired Clients**).

Note To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

3. The client attempts to acquire a DHCP address. The core L2 switch forwards all Auth VLAN traffic to the Out-of-Band Virtual Gateway CAS.
4. The CAS receives the VLAN 100 traffic on its untrusted interface (via the 802.1q trunk).
5. With VLAN mapping rules already configured to map the Auth VLAN to the Access VLAN (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**), the CAS retags the allowed DHCP traffic from VLAN 100 on its untrusted side to VLAN 10 on its trusted side and forwards the retagged traffic on its trusted interface to the L3 router/DHCP server.

Note When the CAS is a Virtual Gateway, it can only be in DHCP Passthrough mode. When VLAN mapping is used for Out-of-Band, the default permissions on the filters transparently allow DNS and DHCP traffic from the untrusted interface, and no additional traffic control policies need to be configured. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details on VLAN mapping.

6. From the router's point of view, this is a request from VLAN 10. The router returns the DHCP response to VLAN 10 on the CAS.
7. With VLAN mapping rules enabled, the CAS retags the allowed traffic (on the 802.1q trunk) from VLAN 10 to VLAN 100 and forwards the DHCP response to the initiating client.
8. The client authenticates through the Clean Access Server via web login or the Agent. If configured, the client goes through posture assessment, all the while transmitting and receiving traffic on the Auth VLAN (100) to the CAS. All traffic that is permitted for remediation is allowed to pass through the CAS, and is placed on VLAN 10. If the traffic is not permitted, it is dropped. When certified, the client is placed on the Certified Devices List.
9. At this point, CAM sends an SNMP SET trap to the switch instructing it to change the client port from the Auth VLAN (100) to the Access VLAN (10) (as specified in the Port Profile), and puts the MAC address of the client in the OOB Online Users list (**Monitoring > Online Users > View Online Users > Out-of-Band**).
10. Because this is an OOB Virtual Gateway deployment, and the client already has an IP address associated with the Access VLAN, the client port is not bounced after it is switched to the Access VLAN.
11. Once the client is on the Access VLAN, the client is on the trusted network and the client's traffic no longer goes through the Clean Access Server.

Note If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to "kick" the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see Configure Access to Authentication VLAN Change Detection, page 3-67.

12. For certified clients, the Port Profile form (**OOB Management > Profiles > Port > New** or **Edit**) provides the following options (see Add Port Profile, page 3-34 for details). You can switch the client to:

- The Access VLAN specified in the Port Profile form.
- The Access VLAN specified for the *user role* of the client, if you choose to use a role-based port profile (see Figure 3-9 on page 3-27 for details).
- The initial VLAN of the port. For this configuration, the client port is switched to the Auth VLAN for authentication/certification, then when the client is certified, the port is switched back to the initial VLAN of the port saved by the CAM when the switch was added.

Note also that:

- If the client's MAC address is on the Certified Devices List, but not on the Out-of-Band Online Users list (in other words, the client is certified but logged off the network), you can keep the client on the Access VLAN at the next login (allowing trusted network access), or you can put the client on the Authentication VLAN at the next login to force the user to re-authenticate through the CAS. Because the client is already certified, the client does not go through Nessus Scanning, only posture assessment.
- Removing an OOB client from the Certified Devices List removes the Out-of-Band user from the Out-of-Band Online Users list. You can optionally configure the port also to be bounced.
- Client machine shutdown/reboot will trigger a linkdown trap (if set up on the switch) sent from the switch to the CAM. The behavior of the client (Agent or web login) depends on the Port Profile setting for that specific port.
- If the CAM is down and the CAS is performing VLAN mapping in "fail open" state, do not reboot the CAS because the VLAN mapping capability will be lost until the CAM comes back online.

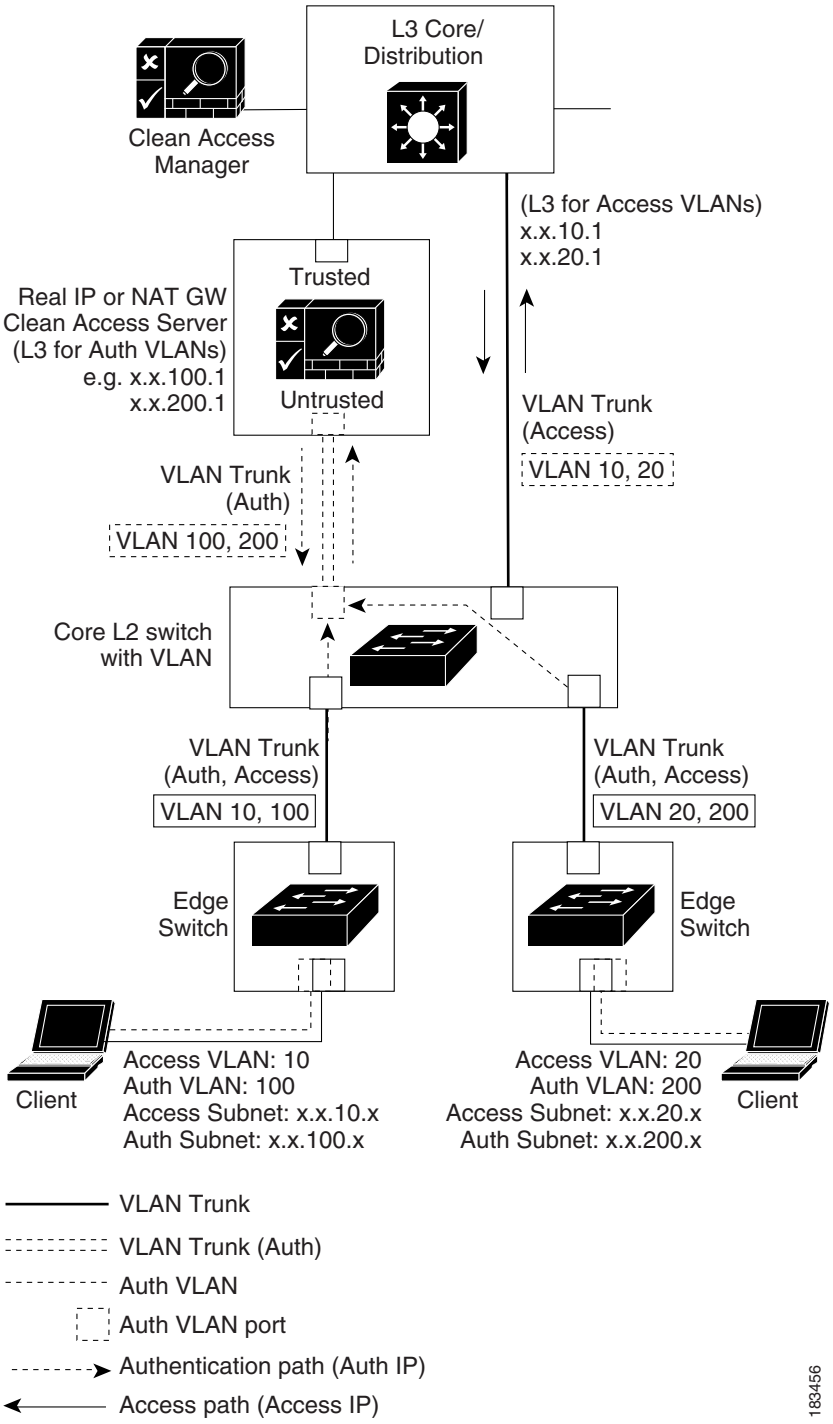
For additional configuration information, see the "Understanding VLAN Settings" and "VLAN Mapping in Virtual Gateway Mode" sections of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Out-of-Band Real-IP Gateway Deployment

In Out-of-Band Real-IP gateway deployment, the client IP address has to change when the port is changed from the Auth VLAN to the Access VLAN.

Figure 3-4 illustrates the sequence described below. In this example, the Authentication VLAN is 100, and the Access VLAN is 10.

Figure 3-4 Out-of-Band Real-IP Gateway Deployment



Flow for Out-of-Band Real-IP Gateway Mode

1. The unauthenticated user connects the client machine to the network through an edge switch.
2. The switch sends MAC notification or linkup/linkdown SNMP traps for the client to the CAM. Because the client is not on the Certified Devices List/Online Users list yet, the CAM sends an SNMP SET trap to the switch instructing it to change the client port to the Authentication VLAN specified in the Port Profile (100), and the CAM places the client on the Out-of-Band Wired Clients list (**OOB Management > Devices > Discovered Clients > Wired Clients**).

Note To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

3. The unauthenticated client requests and receives an IP address on the Auth VLAN (x.x.100.x).
4. The client authenticates through the CAS via web login or the Agent. If configured, the client goes through posture assessment, all the while transmitting and receiving traffic on the Auth VLAN (100) to the CAS. When clean, the client is placed on the Certified Devices List. The CAS acts as the default gateway while the client remediates. Only permitted traffic is allowed to pass through from the untrusted to trusted interface.
5. At this point, the CAM instructs the switch to change the client switch port from the Authentication VLAN (100) to the Access VLAN (10) (according to the Port Profile), and puts the client MAC address on the Out-of-Band Online Users list (**Monitoring > Online Users > View Online Users > Out-of-Band**).
6. The client port is switched to the Access VLAN and is bounced (as set in the Port Profile). When the port is bounced, the client acts as if the network cable is unplugged, thus releasing its DHCP binding on the interface. Once the port is brought back up from the shutdown state, the client performs a DHCP renewal or discovery, as if it were connecting to the network for the first time. Since the switch port is now on a different VLAN, the client receives a new IP address that is valid for the access subnet.
7. With an IP address on the Access VLAN (x.x.10.x), the client now transmits traffic on the trusted network, on the Access VLAN specified in the Port Profile.
8. Once the client is on the Access VLAN, the client's traffic no longer goes through the CAS.

Note If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to "kick" the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see Configure Access to Authentication VLAN Change Detection, page 3-67.

9. For certified clients, the Port Profile form (**OOB Management > Profiles > Port > New/Edit**) provides the following options (see Add Port Profile, page 3-34). You can switch the client to:

- The Access VLAN specified in the Port Profile form.
- The Access VLAN specified for the *user role* of the client, if you choose to use a role-based port profile (see Figure 3-9 on page 3-27 for details).

- The initial VLAN of the port. For this configuration, the client port is switched to the Authentication VLAN for authentication/certification, then when the client is certified, the port is switched back to the initial VLAN of the port saved by the CAM when the switch was added.

Note

- If the client's MAC address is on the Certified Devices List, but not on the Out-of-Band Online Users list (in other words, the client is certified but logged off the network), you can keep the client on the Access VLAN at the next login (allowing trusted network access), or you can put the client on the Authentication VLAN at the next login to force the user to re-authenticate through the CAS. Because the client is already certified, the client does not go through Nessus Scanning, only posture assessment.
- Removing an OOB client from the Certified Devices List removes the Out-of-Band user from the Out-of-Band Online Users list and bounces the port. You can optionally configure the Port Profile not to bounce the port.

L3 Out-of-Band Deployment

For details on L3 OOB, refer to the following sections:

- Enable Web Client for Login Page, page 5-5
- "Configuring Layer 3 Out-of-Band (L3 OOB)" in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Configure Your Network for Out-of-Band

The Clean Access Manager (CAM) manages Out-of-Band Clean Access Servers (CASs) and switches through the admin network. The trusted interface of the CAS connects to the admin/management network, and the untrusted interface of the CAS connects to the managed client network.

When a client connects to a managed port on a managed switch, the port is set to the authentication VLAN and the traffic to/from the client goes through the Clean Access Server. After the client is authenticated and certified through the Clean Access Server, the port connected to the client is changed to the access VLAN. Once on the access VLAN, traffic to and from certified clients bypasses the Clean Access Server.

In most OOB deployments (except L2 OOB Virtual Gateway where the Default Access VLAN is the Access VLAN in the Port profile), the client needs to acquire a different IP address from the Access VLAN after posture assessment.

For Real-IP Gateway setup, the client port is bounced to prompt the client to acquire a new IP address from the admin/access VLAN.

The next sections describe the configuration steps needed to set up your OOB deployment:

- Configure Your Switches, page 3-14
- Configure OOB Switch Management on the CAM, page 3-25
- Configure Access to Authentication VLAN Change Detection, page 3-67

Note If configuring the CAS as an OOB Virtual Gateway, do not connect the untrusted interface to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

Configure Your Switches

This section describes the steps needed to set up switches to be used with Cisco NAC Appliance Out-of-Band.

- Configuration Notes, page 3-14
- Example Switch Configuration Steps, page 3-15
- OOB Network Setup/Configuration Worksheet, page 3-21
- List of MIBs and OIDs, page 3-22

Configuration Notes

The following considerations should be taken into account when configuring switches for OOB:

- Because Cisco NAC Appliance OOB can control switch trunk ports, ensure the uplink ports for managed switches are configured as “unmanaged” ports after upgrade. This can be done in one of two ways:
  - Before upgrade, change the **Default Port Profile** for the entire switch to “unmanaged” (see Config Tab, page 3-63).
  - After upgrade, change the **Profile** for the applicable uplink ports of the switch to “unmanaged” (see Ports Management Page, page 3-54).

  This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.
- Cisco NAC Appliance OOB supports 3750 StackWise technology. With stacks, when MAC notification is used and there are more than 252 ports on the stack, MAC notification cannot be set/unset for the 252nd port using the CAM. There are two workarounds:
  - Use linkup/linkdown SNMP notifications only
  - If using MAC notification, do not use the 252nd port and ignore the error; other ports will work fine
- Switch clusters are not supported. As a workaround, assign an IP address to each switch.
- The ifindex persistence must be enabled on the switches. You can configure it by using the following command:

  ```
  (config)# snmp ifmib ifindex persist
  ```

- Cisco recommends turning on portfast on access ports (those directly connected to client machines).
- Cisco recommends setting the mac-address aging-time to a minimum of 3600 seconds.
- On some models of Cisco switches (e.g. 4507R, IOS Version 12.2(18) EW), the MAC address(es) connected to a particular port may not be available after Port Security is enabled.

- If implementing High-Availability, do not enable Port Security on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.
- You must ensure your switch has the Access VLAN in its VLAN database to ensure proper switching behavior. On some models of Cisco switches (e.g. 6506, IOS Version 12.2(18) SXD3), MAC address(es) connected to a particular port may not be available when the Access VLAN of the port does not exist in the VLAN database.
- Only Ethernet (Fa, Gi, fiber) port types (reported by SNMP) are displayed.
- If no healthy Clean Access Manager is in service, ports remain in the VLAN they are in until connectivity to the CAM is restored.
- For SNMP V3, each switch to be managed by the CAM must have unique Engine ID.
- The syntax for "mac-address notification" commands varies for different switch versions. When a switch is upgraded, the change in the syntax should be evaluated. The modified commands should be re-applied to the switch configuration after upgrading and reloading the switch.

Example Switch Configuration Steps

Step 1 Connect the machines and switches. Write down the admin VLAN, Access VLAN, Authentication VLAN and other information (see Table 3-2 for a detailed list).

Clean Access Manager (CAM):	172.16.1.61
CAM management VLAN:	VLAN 2
Clean Access Server (CAS):	10.60.3.2
CAS management VLAN:	VLAN 3
Access VLANs:	10, 20
Authentication VLANs:	31, 41
Switch (Catalyst 2950):	172.16.1.64

The trusted interface of the CAS is connected to the trunk port for Access VLANs 10, 20 and the untrusted interface of the CAS is connected to the trunk port for Auth VLANs 31, 41.

Refer the switch documentation for details on configuring your specific switch model.

Step 2 Configure the switch IP address (172.16.1.64) and Access VLANs (10, 20).

Step 3 When using Virtual Gateway with VLAN mapping, make sure there is no VLAN interface for any of the Auth VLANs on your existing Layer 3 switch or router (e.g. CAT 6500). For example, for an Access VLAN 10 and Auth VLAN 31 for which VLAN mapping has been configured on the CAS, and if an interface already exists on the L3 switch/router for the Auth VLAN, you can turn it off using the following commands:

```
(config)# no int vlan 31
(config)# vlan 31
```

The first command turns off the interface and the second ensures VLAN 31 (Auth VLAN) is in the VLAN database table.You will also need to Enable VLAN Mapping in the CAS as described in Figure 3-8 on page 3-27.

Note If the CAM is down and the CAS is performing VLAN mapping in "fail open" state, do not reboot the CAS because the VLAN mapping capability will be lost until the CAM comes back online.

Step 4 For Real-IP Gateways, add static routes on the L3 switch or router to route traffic for the managed subnets to the trusted interface of the respective CASs.

Step 5 Configure SNMP miscellaneous settings:

```
(config)# snmp-server location <location_string>
(config)# snmp-server contact <admin_contact_info>
```

Note When configuring SNMP settings on switches, never use the "@" character in the community string.

Step 6 Configure the SNMP read community string (V1/V2c) or username/password (V3) used in Configure Switch Profiles, page 3-30.

- SNMP V1/V2c settings (SNMP read-only community string is "c2950_read"):

  ```
  (config)# snmp-server community c2950_read RO
  ```

- SNMP V3 settings (username: "c2950_user;" password: "c2950_auth"):

  ```
  (config)# snmp-server view v1default iso included
  (config)# snmp-server group c2950_group v3 auth read v1default write v1default
  (config)# snmp-server user c2950_user c2950_group v3 auth md5 c2950_auth
  ```

  For SNMP V3 read, create SNMP V3 contexts for the VLANs that are used in the switch. To get the contexts that are present in the switch, run the following command in the switch:

  ```
  access-switch# sh snmp context
  ```

  The output will be similar to the following:

  ```
  vlan-1
  vlan-2
  vlan-3
  vlan-8
  vlan-9
  ....
  ....
  vlan-1005
  ```

  Create SNMP V3 contexts for the VLANs that are used. For example, if the **`vlan-8`** and **`vlan-9`** are being used, then the command to create the context is as follows:

  ```
  (config)# snmp-server group c2950_group v3 auth context vlan-8
  (config)# snmp-server group c2950_group v3 auth context vlan-9
  ```

  The above example is to create SNMP V3 context when the security method is set to **AuthNoPriv**. You need to provide the commands based on the security level as follows:

  - **auth** — AuthNoPriv as security level
  - **noauth** — NoAuthNoPriv as security level
  - **priv** — AuthPriv as security level

Step 7 Configure the SNMP write community string (V1/V2c) or username/password (V3) used in Configure Switch Profiles, page 3-30.

- SNMP V1/V2c settings (SNMP read-write community string is "c2950_write"):

```
(config)# snmp-server community c2950_write RW
```

- SNMP V3 settings:

  For auth (username: “c2950_user;” password: “c2950_auth”):

  ```
  (config)# snmp-server view v1default iso included
  (config)# snmp-server group c2950_group v3 auth read v1default write v1default notify
  vldefault
  (config)# snmp-server user c2950_user c2950_group v3 auth md5 c2950_auth
  ```

  For priv (username: “c2950_user;” password: “c2950_priv”):

  ```
  (config)# snmp-server view v1default iso included
  (config)# snmp-server group c2950_group v3 priv read v1default write v1default notify
  vldefault
  (config)# snmp-server user c2950_user c2950_group v3 auth md5 c2950_auth priv des
  c2950_ priv
  ```

Step 8 Enable MAC notification or linkup/linkdown SNMP traps and set MAC address table aging-time when necessary for the switch.

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps. If enabling MAC notification traps, the MAC address table aging-time must be set to a non-zero value. Cisco recommends setting the MAC address table aging-time to at least 3600 seconds for switches that have limited space for MAC addresses, and to a higher value (e.g. 1000000) if your switches support a sufficiently large number of MAC entries. If a switch supports MAC notification traps, Cisco NAC Appliance uses the MAC change notification/MAC move notification trap by default, in addition to linkdown traps (to remove users). If the switch does not support MAC change notification/MAC move notification traps, the Clean Access Manager uses linkup/linkdown traps only.

```
(config)# snmp-server enable traps mac-notification
(config)# snmp-server enable traps snmp linkup linkdown
(config)# mac-address-table aging-time 3600
```

Step 9 Enable the switch to send SNMP MAC notification and linkup traps to the Clean Access Manager. The switch commands used here depend on the SNMP version used in the SNMP trap settings in Configure SNMP Receiver, page 3-44.

Note For better security, Cisco recommends administrators use SNMP V3 and define ACLs to limit SNMP write access to the switch.

To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- SNMP v1 (SNMP community string is “cam_v1”):

  ```
  (config)# snmp-server host 172.16.1.61 traps version 1 cam_v1 udp-port 162
  mac-notification snmp
  ```

- SNMP V2C (SNMP community string is “cam_v2”):

  ```
  (config)# snmp-server host 172.16.1.61 traps version 2c cam_v2 udp-port 162
  mac-notification snmp
  ```

- SNMP v3.
- The following commands should be run in the order of: group, user, and host.

For auth (SNMP username/password is “cam_user”/“cam_auth”)

```
(config)# snmp-server group cam_group v3 auth read v1default write v1default notify
v1default
(config)# snmp-server user cam_user cam_group v3 auth md5 cam_auth
(config)# snmp-server host 172.16.1.61 traps version 3 auth cam_user udp-port 162
mac-notification snmp
```

For priv (SNMP username/password is “cam_user”/“cam_priv”)

```
(config)# snmp-server group cam_group v3 priv read v1default write v1default notify
v1default
(config)# snmp-server user cam_user cam_group v3 auth md5 cam_auth priv des cam_priv
(config)# snmp-server host 172.16.1.61 traps version 3 priv cam_user udp-port 162
mac-notification snmp
```

Step 10 Enable the Port Fast command to bring a port more quickly to a Spanning Tree Protocol (STP) forwarding state. You can do this at the switch configuration level for all interfaces, or at the interface configuration level for each interface:

- Switch configuration level:

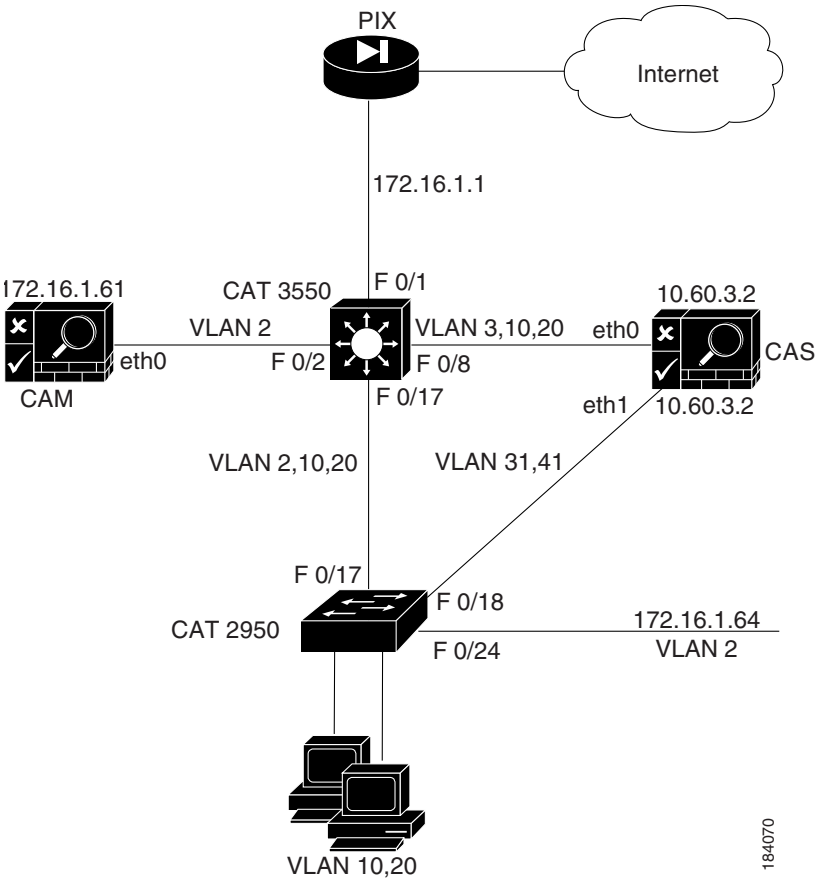
  ```
  (config)# spanning-tree portfast default
  ```

- Interface configuration level:

  ```
  (config-if)# spanning-tree portfast
  ```

Figure 3-5 illustrates an example OOB setup.

Figure 3-5 Example Physical Setup



Note The CAS interfaces should be on a separate VLAN from the CAM VLAN and access VLANs.

Figure 3-6 Example L3 Switch Configuration

```
!To PIX
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
! To Manager
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
switchport trunk native vlan 999
 switchport trunk allowed vlan 3,10,20
 switchport mode trunk
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,10,20
 switchport mode trunk
!
interface VLAN1
 ip address 192.168.1.61 255.255.255.0
 shutdown
!
interface VLAN2
 ip address 172.16.1.60 255.255.255.0
!
interface VLAN3
 ip address 10.60.3.1  255.255.255.0

interface VLAN10
 ip address 10.60.10.1 255.255.255.0
!
interface VLAN20
 ip address 10.60.20.1 255.255.255.0
!!
ip default-gateway 172.16.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
ip http server
!
```

Note: No int vlan 31 or 41

184141

OOB Network Setup/Configuration Worksheet

Table 3-2 summarizes information needed to configure switches and the Clean Access Manager.

Table 3-2 Configuration Worksheet

Configuration Settings	Value
Switch Configuration	
Switch IP Address:	
Access VLANs:	
Auth VLANs:	
location_string:	
admin_contact_info:	
SNMP version used:	
SNMP (V1/V2c) read community string:	
SNMP (V1/V2c) write community string:	
SNMP (V3) auth method/ username/password:	
MAC notification or linkup:	
SNMP Trap V1/V2c community string, or SNMP Trap V3 auth method/usr/pwd (to send traps to CAM):	
CAM/CAS Configuration	
CAM IP address:	
CAS Trusted IP address:	
CAS Untrusted IP address:	
CAM VLAN (management):	
CAS VLAN (management):	
CAM SNMP Trap Receiver:	
Community string for SNMP Trap V1 switches:	
Community string for SNMP Trap V2c switches:	
Auth method/username/password for SNMP Trap V3 switches:	

List of MIBs and OIDs

Table 3-3 lists the MIBs and OIDs used by NAC for both wireless controllers and switches.These OIDs and their corresponding MIBs should be implemented by the device that is being added to NAC.

Table 3-3 List of MIBs and OIDs used by NAC

OID	Object Name	MIB
1.3.6.1.2.1.2.1.0	ifNumber	IF-MIB
1.3.6.1.2.1.2.2.1.1	ifIndex	IF-MIB
1.3.6.1.2.1.2.2.1.2	ifDescr	IF-MIB
1.3.6.1.2.1.31.1.1.1.1	ifName	IF-MIB
1.3.6.1.2.1.2.2.1.3	ifType	IF-MIB
1.3.6.1.2.1.2.2.1.7	ifAdminStatus	IF-MIB
1.3.6.1.2.1.2.2.1.8	ifOperStatus	IF-MIB
1.3.6.1.6.3.1.1.5.3	Linkdown	IF-MIB
1.3.6.1.6.3.1.1.5.4	Linkup	IF-MIB
1.3.6.1.2.1.2.2.1.6	ifPhysAddress	IF-MIB
1.3.6.1.2.1.47.1.2.1.1.4	entLogicalCommunity	ENTITY-MIB
1.3.6.1.2.1.47.1.2.1.1.3	entLogicalType	ENTITY-MIB
1.3.6.1.2.1.17.4.3.1.2	dot1dTpFdbPort	BRIDGE-MIB
1.3.6.1.2.1.17.4.3.1.3	dot1dTpFdbStatus	BRIDGE-MIB
1.3.6.1.2.1.17.1.4.1.2	dot1dBasePortIfIndex	BRIDGE-MIB
1.3.6.1.2.1.17	dot1dBridge	BRIDGE-MIB
1.3.6.1.4.1.9.9.68.1.2.2.1.2	vmVlan	CISCO-VLAN-MEMBERSHIP MIB
1.3.6.1.4.1.9.9.46.1.3.1.1.2	vtpVlanState	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.6.1.1.5	vlanTrunkPortNativeVlan	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.6.1.1.14	vlanTrunkPortDynamicStatus	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.6.1.1.4	vlanTrunkPortVlansEnabled	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.6.1.1.17	vlanTrunkPortVlansEnabled2k	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.6.1.1.18	vlanTrunkPortVlansEnabled3k	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.6.1.1.19	vlanTrunkPortVlansEnabled4k	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.3.1.1.4	vtpVlanName	CISCO-VTP-MIB
1.3.6.1.4.1.9.9.173.1.2.1.1.1	cpvlanPrivatePortSecondaryVlan	CISCO-PRIVATE-VLAN-MIB
1.3.6.1.4.1.9.9.215.1.1.1.0	cmnGlobalFeatureEnabled	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.1.2.0	cmnNotificationInterval	CISCO-MAC-NOTIFICATION MIB

Table 3-3 List of MIBs and OIDs used by NAC

OID	Object Name	MIB
1.3.6.1.4.1.9.9.215.1.1.5.0	cmnNotificationsEnabled	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.2.1.1	cmnIfConfigEntry	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.2.1.1.1	cmnMacAddrLearntEnable	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.2.1.1.2	cmnMacAddrRemovedEnable	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.1.8.1.2	cmnHistMacChangedMsg	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.2.0.1	cmnMacChangedNotification	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.2.0.2	cmnMacMoveNotification	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.3.3	cmnMACMoveAddress	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.3.4	cmnMACMoveVlanNumber	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.3.5	cmnMACMoveFromPortId	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.215.1.3.6	cmnMACMoveToPortId	CISCO-MAC-NOTIFICATION MIB
1.3.6.1.4.1.9.9.315.1.2.1.1.1	cpsIfPortSecurityEnable	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.2.1.1.2	cpsIfPortSecurityStatus	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.2.1.1.7	cpsIfStaticMacAddrAgingEnable	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.2.1.1.8	cpsIfViolationAction	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.2.1.1.10	cpsIfSecureLastMacAddress	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.2.1.1.11	cpsIfClearSecureAddresses	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.2.2.1.2	cpsSecureMacAddrType	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.2.2.1.4	cpsSecureMacAddrRowStatus	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.9.315.1.1.3.0	cpsGlobalPortSecurityEnable	CISCO-PORT-SECURITY-MIB
1.3.6.1.4.1.9.2.1.54.0	writeMem	OLD-CISCO-SYS-MIB
1.3.6.1.4.1.9.9.656.1.4.1.1.2	cafSessionClientMacAddress	CISCO-AUTH-FRAMEWORK MIB
1.3.6.1.4.1.9.9.656.1.4.1.1.20	cafSessionReauth	CISCO-AUTH-FRAMEWORK MIB
1.3.6.1.2.1.1.2.0	Sysobjectid	SNMPv2-MIB
1.3.6.1.2.1.1.6.0	sysLocation	SNMPv2-MIB
1.3.6.1.6.3.1.1.4.1	snmpTrapOID	SNMPv2-MIB

Table 3-3 List of MIBs and OIDs used by NAC

OID	Object Name	MIB
1.3.6.1.2.1.1.4.0	sysContact	SNMPv2-MIB
1.3.6.1.2.1.4.20.1.1	ipAdEntAddr	IP-MIB
1.3.6.1.2.1.4.20.1.2	ipAdEntIfIndex	IP-MIB
1.3.6.1.2.1.4.20.1.3	ipAdEntNetMask	IP-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1.11	cldcClientEntry	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.0	ciscoLwappDot11ClientMIBNotifs	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.0.2	OID_CLDC_ASSOC	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.0.3	OID_CLDC_DISASSOC	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1.1	cldcClientMacAddress	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1.3	cldcClientWlanProfileName	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1.8	cldcApMacAddress	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1.10	OID_CLDC_CLIENT_IP	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1.12	OID_CLDC_AUTH_VLAN	CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1.13	OID_CLDC_ACCESS_VLAN	CISCO-LWAPP-DOT11-CLIENT-MIB

Configure OOB Switch Management on the CAM

This section describes the web admin console configuration steps to implement Out-of-Band. In general, you first configure Group, Switch, and Port profiles, as well as the Clean Access Manager's SNMP Receiver settings, under **OOB Management > Profiles**. After profiles are configured, add the switches you want to control to the Clean Access Manager's domain under **OOB Management > Devices**, and apply the profiles to the switches.

After switches are added, the ports on the switch are discovered, and the **Port** and **Config** icons and pages for each switch appear on **OOB Management > Devices > Devices > List**.

Clicking the manage **Ports** icon brings up the **Ports** tab. The **Ports** page is where you apply a managed Port Profile to a specific port(s) to configure how a client's traffic is temporarily routed through the CAS for authentication/certification before being allowed on the trusted network.

The configuration sequence is as follows:

1. Plan your settings and configure the switches to be managed, as described in previous section, Configure Your Switches, page 3-14
2. Add Out-of-Band Clean Access Servers and Configure Environment, page 3-25
3. Configure Global Device Filters to Ignore IP Phone MAC Addresses, page 3-28
4. Configure Group Profiles, page 3-28
5. Configure Switch Profiles, page 3-30
6. Configure Port Profiles, page 3-33
7. Configure VLAN Profiles, page 3-40
8. Configure SNMP Receiver, page 3-44
9. Add and Manage Switches, page 3-48
10. Manage Switch Ports, page 3-54

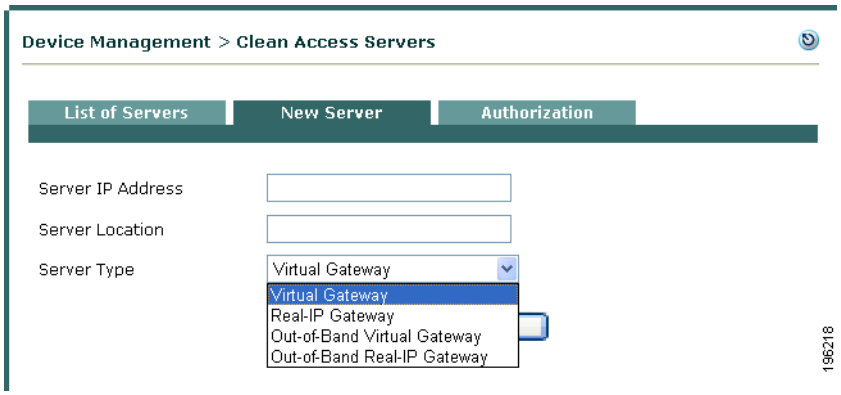
Add Out-of-Band Clean Access Servers and Configure Environment

Note In order to establish the initial secure communication channel between a CAM and CAS, you must import the root certificate from each appliance into the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.

Almost all the CAM/CAS configuration for Out-of-Band deployment is done directly in the **OOB Management** module of the web admin console. Apart from the **OOB Management** module configuration, OOB setup is almost exactly the same as traditional In-Band setup, except for the following differences:

Step 1 Choose an Out-of-Band gateway type when you add your Clean Access Server(s) (Figure 3-7).

Figure 3-7 Add New OOB Server



The Out-of-Band **Server Types** appear in the dropdown menu to add a new Clean Access Server:

- Out-of-Band Virtual Gateway
- Out-of-Band Real-IP Gateway

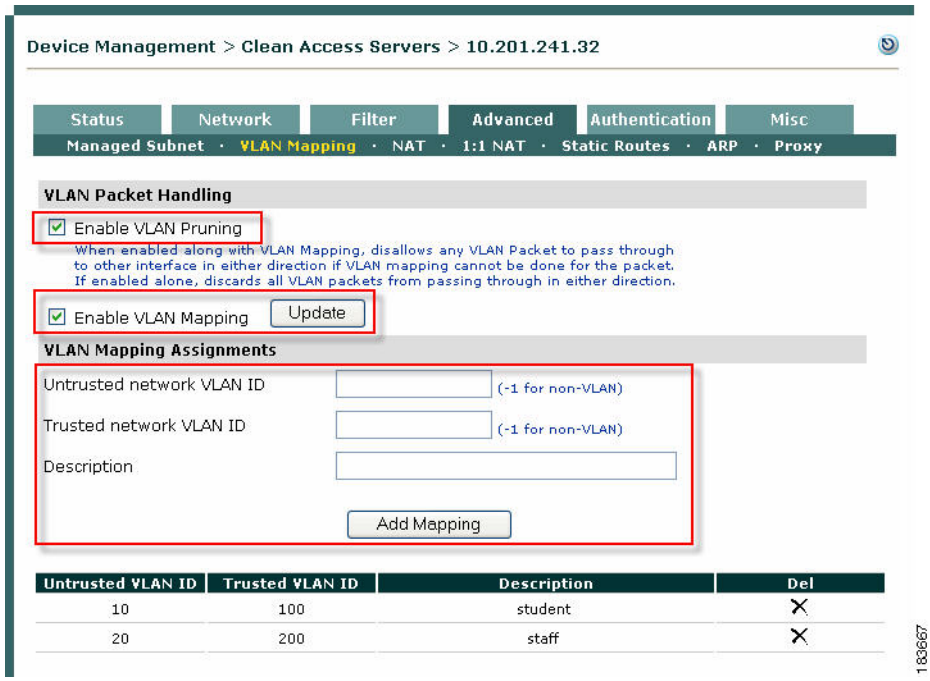
  The Clean Access Server itself must be ***either*** In-Band or Out-of-Band. The Clean Access Manager can control both In-Band and Out-of-Band CASs in its domain.

Note

- For Virtual Gateway (In-Band or OOB), do not connect the untrusted interface (eth1) of the CAS to the switch until **after** the CAS has been added to the CAM via the web console.
- For Virtual Gateway with VLAN mapping (In-Band or OOB), do not connect the untrusted interface (eth1) of the CAS to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

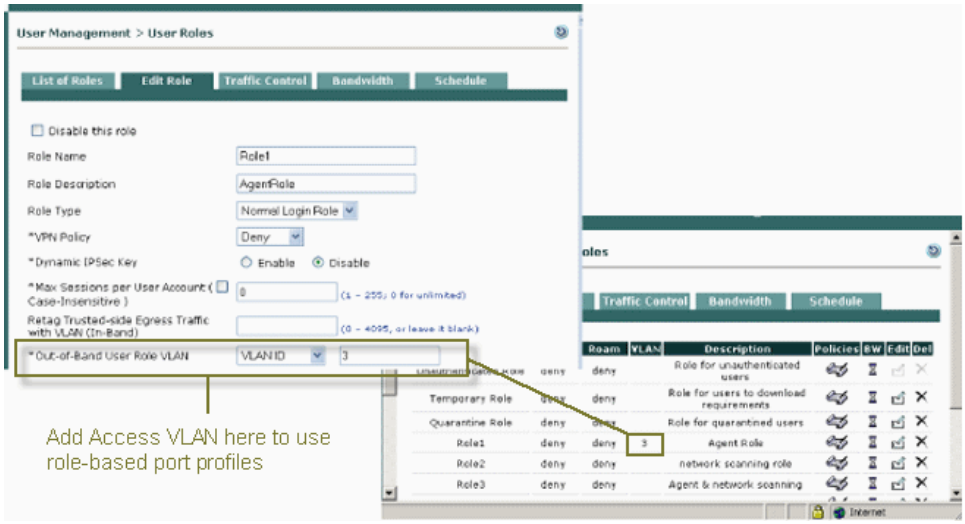
Step 2 For OOB Virtual Gateways, you must enable and configure VLAN mapping (Figure 3-8) on the CAS for each Auth/Access VLAN pair configured on the switch. This is required in order to retag an unauthenticated client's allowed traffic (e.g. DHCP/DNS) from the Auth VLAN to the Access VLAN (and vice-versa). You can also enable VLAN pruning for CAS appliances operating in Virtual Gateway mode. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for further details on VLAN mapping and VLAN pruning.

Figure 3-8 Enable VLAN Mapping for Out-of-Band Virtual Gateways



Step 3 If you plan to use role-based port profiles (see Configure Port Profiles, page 3-33), specify the Access VLAN in the **Out-of-Band User Role VLAN** field when you create a new user role (Figure 3-9). See Adding a New User Role, page 6-7 for details.

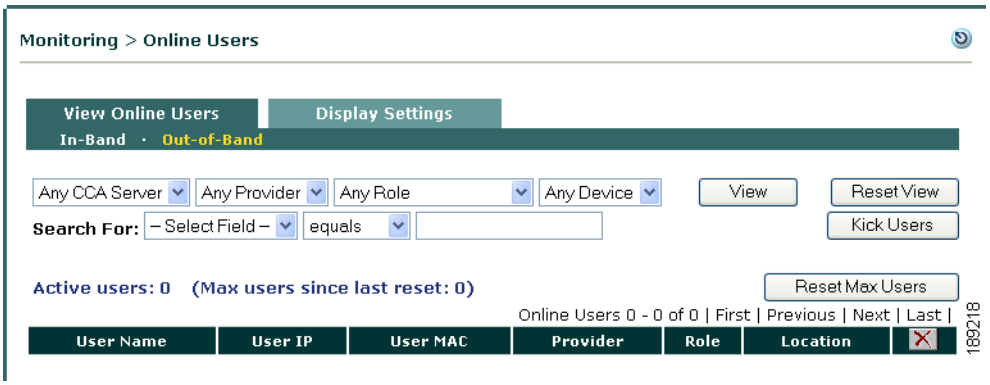
Figure 3-9 Configure User Role with Access VLAN



Note You can specify a VLAN Name or VLAN ID in the Port Profile or for the Out-of-Band User Role VLAN. You can specify only numbers for VLAN ID. VLAN Name is case-sensitive, but you can specify wildcards for a VLAN Name. The switch will use the first match for the wildcard VLAN Name.

Step 4 When Out-of-Band is enabled, the **Monitoring > View Online Users** page displays links for both **In-Band** and **Out-of-Band** users and display settings (Figure 3-10). See Out-of-Band Users, page 11-31 for details.

Figure 3-10 View Out-of-Band Online Users



Configure Global Device Filters to Ignore IP Phone MAC Addresses

An important feature of any OOB configuration is to ensure IP phones through which client machines connect to the network do not inadvertently terminate the client connection when MAC notification events from the IP phone initiate a change in the network connection like a VLAN change. To do this:

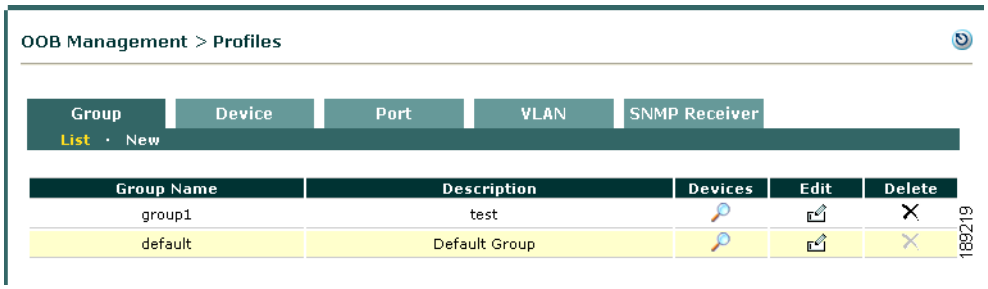
- Configure a global Device Filter (**Device Management > Filters > Devices > New** or **Edit**) with the "Ignore" option for the IP phone MAC address to ensure Cisco NAC Appliance ignores SNMP trap events from the IP phone
- Enable the **Change VLAN according to global device filter list** option when you configure the Port Profile, as described in Add Port Profile, page 3-34.

For more information, see Device Filters for Out-of-Band Deployment Using IP Phones, page 2-15. For detailed configuration instructions, see Add Global Device Filter, page 2-20.

Configure Group Profiles

When you first add a switch to the Clean Access Manager's domain (under **OOB Management > Devices**), a Group profile must be applied to add the new switch. There is a predefined Group profile called **default**, shown in Figure 3-11. All switches are automatically put in the **default** group when you add them. You can leave this default Group profile setting, or you can create additional Group profiles as needed. If you are adding and managing a large number of switches, creating multiple Group profiles allow you to filter which sets of devices to display from the list of switches (under **OOB Management > Devices > Devices > List**).

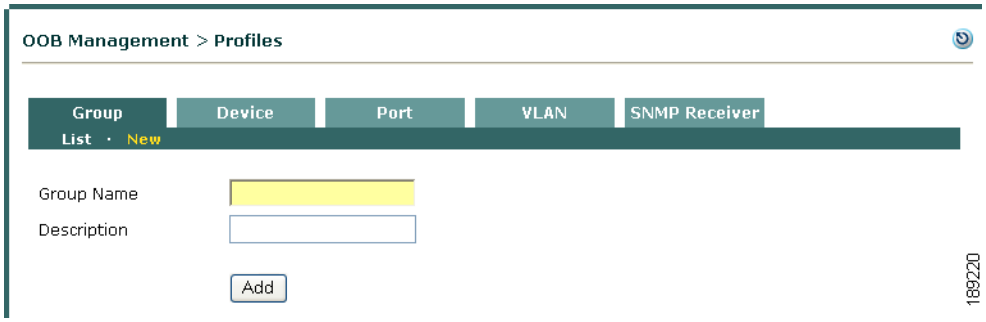
Figure 3-11 Group Profiles List



Add Group Profile

Step 1 Go to **OOB Management > Profiles > Group > New** (Figure 3-12).

Figure 3-12 New Group



Step 2 Enter a single word for the **Group Name**. You can use digits and underscores, but no spaces.

Step 3 Enter an optional **Description**.

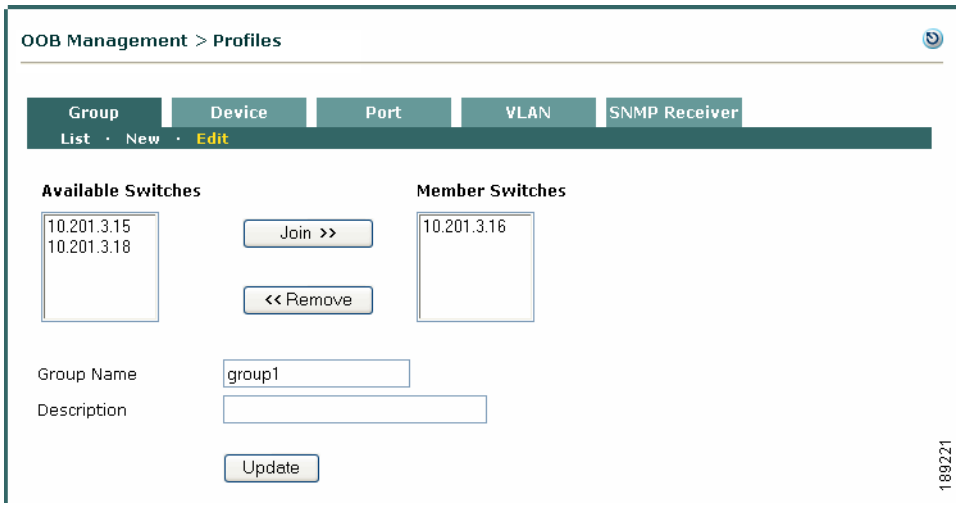
Step 4 Click **Add**. The new Group profile appears under **OOB Management > Profiles > Group > List**.

Edit Group Profile

Step 1 To edit the profile later, after actual switches are added, go to **OOB Management > Profiles > Group > List** and click the **Edit** icon for the new Group profile.

Step 2 The **Edit** page appears (Figure 3-13).

Figure 3-13 Edit Group



Step 3 You can toggle the switches that belong in the Group profile by selecting the IP address of the switch from the **Member Switches** or **Available Switches** columns and clicking the **Join** or **Remove** buttons as applicable.

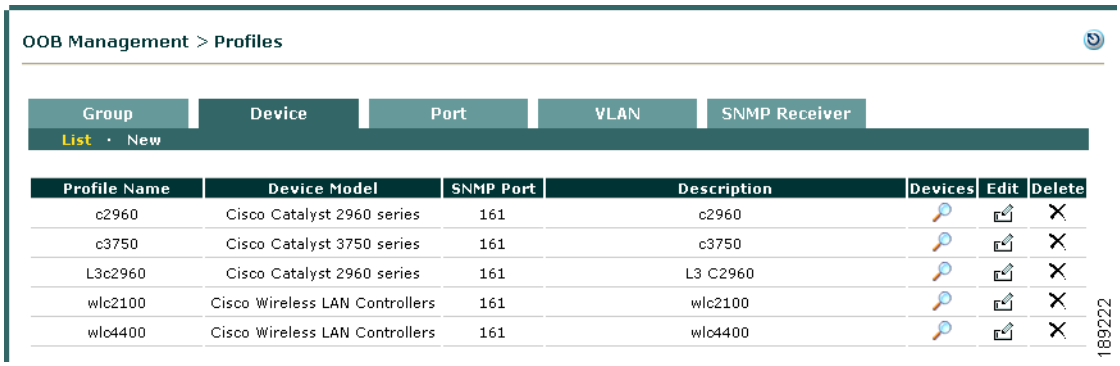
Step 4 Click the **Update** button when done to save your changes.

Note To delete a group profile, you must first remove the joined switches from the profile.

Configure Switch Profiles

A Switch profile must first be created under **OOB Management > Profiles > Device > New**, then applied when a new switch is added. A Switch profile classifies switches of the same model and SNMP settings, as shown in Figure 3-14. The Switch profile configures how the CAM will read/write/change port settings, such as Access/Auth VLAN, on a switch of this particular type.

Figure 3-14 Switch Profiles List



The Switch profiles list under **OOB Management > Profiles > Device > List** provides three icons:

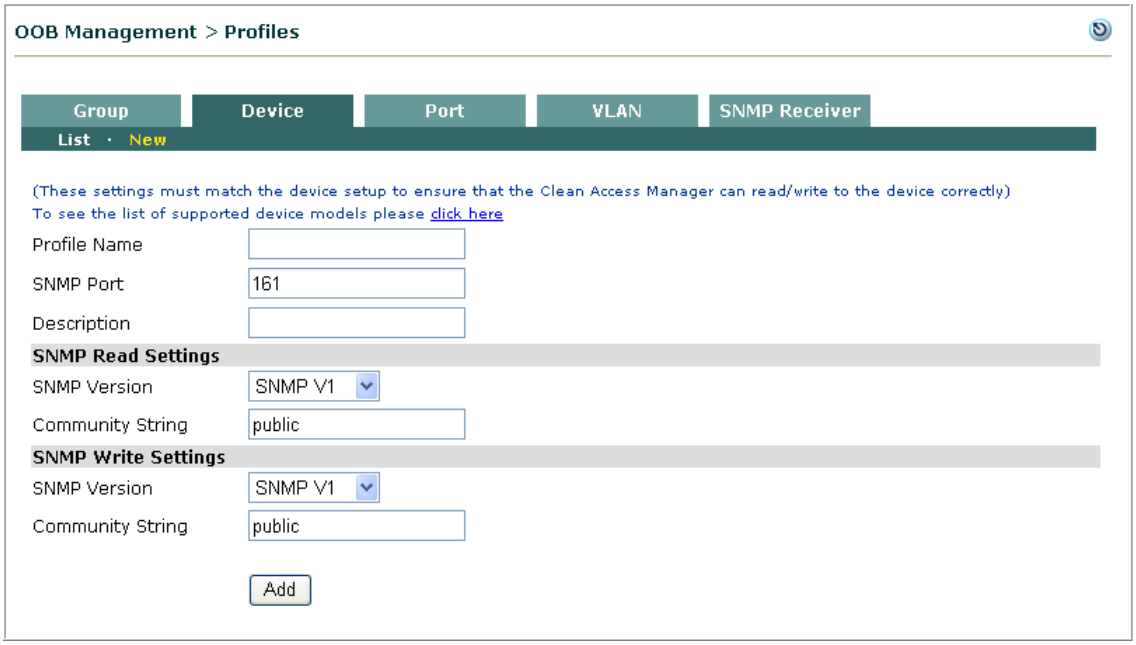
- **Devices**—Clicking this icon brings up the list of added switches and WLCs under **OOB Management > Devices > Devices > List** (see Figure 3-28).
- **Edit**—Clicking this icon brings up the **Edit** Switch profile form (see Figure 3-16).
- **Delete**—Clicking this icon deletes the Switch profile (a confirmation dialog will appear first).

Add Switch Profile

Use the following steps to add a Switch profile.

Step 1 Go to **OOB Management > Profiles > Device > New** (Figure 3-15).

Figure 3-15 New Switch Profile



Step 2 Enter a single word for the **Profile Name**. You can use digits and underscores but no spaces.

Note It is recommended to enter a Switch Profile name that identifies the switch model, and SNMP read and write versions. For example "2950v2v3."

Step 3 Enter the **SNMP Port** configured on the switch to receive read/write requests. The default port is 161 for SNMP GET/SET and the default port is 162 for Traps.

Step 4 Enter an optional **Description**.

Note You can click the link available at the top of this tab to view the list of supported device models.

Step 5 Configure **SNMP Read Settings** to match those on the switch.

- Choose the **SNMP Version**: SNMP V1, SNMP V2C, or SNMP V3.

- Type the **Community String** for SNMP V1 or SNMP V2C configured for the switch.

Step 6 If SNMP V3 is used for SNMP Read Settings on the switch, configure the following settings to match those on the switch:

- Choose a **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES), or AuthPriv(SHA+DES).
- Type the **User Name**.
- Type the **User Auth**.
- Type the **User Priv**.

Step 7 Configure S**NMP Write Settings** to match those on the switch.

- Choose the **SNMP Version**: SNMP V1, SNMP V2C, or SNMP V3.
- Type the **Community String** for SNMP V1 or SNMP V2C configured for the switch.

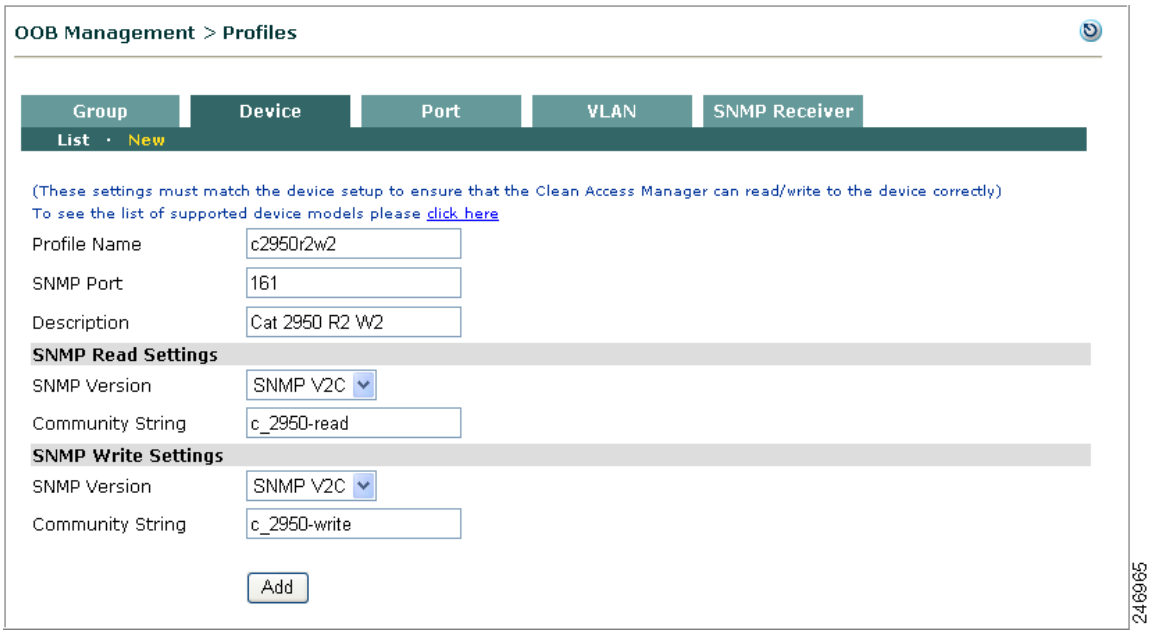
Step 8 If SNMP V3 is used for SNMP write settings on the switch, configure the following settings to match those on the switch:

- Choose a **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES-CBC), or AuthPriv(SHA+DES-CBC).
- Type the **User Name**.
- Type the **User Auth**.
- Type the **User Priv**.

Step 9 Click **Add** to add the Switch profile to **OOB Management > Profiles > Device > List** (Figure 3-28).

Figure 3-16 illustrates a switch profile defining Cisco Catalyst 2950 switches with the same SNMP settings: SNMP V2c with read community string “c2950_read” and write community string “c2950_write.”

Figure 3-16 Example Switch Profile



Configure Port Profiles

The Port profile determines whether a port is managed or unmanaged, the Authentication and Access VLANs to use when switching the client port, and other behavior for the port (see Ports Management Page, page 3-54). There are four types of port profiles for switch ports (shown in Figure 3-17):

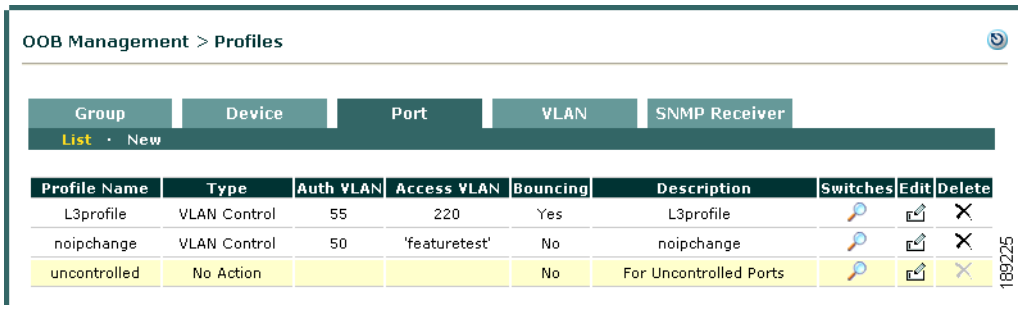
- Unmanaged – For uncontrolled switch ports that are not connected to clients (such as printers, servers, switches, etc.). This is typically the default Port profile.
- Managed with Auth VLAN/Default Access VLAN – Controls client ports using the Auth VLAN and Default Access VLAN defined in the Port profile.
- Managed with Auth VLAN/User Role VLAN – Controls client ports using the Auth VLAN defined in the Port profile and the Access VLAN defined in the user role (see Figure 3-9 on page 3-27).
- Managed with Auth VLAN/ Initial Port VLAN– Controls client ports using the Auth VLAN defined in the Port profile and the Access VLAN defined as the initial port VLAN of the switch port.

Regular switch ports that are not connected to clients use the unmanaged Port profile. Client-connected switch ports use managed Port profiles. When a client connects to a managed port, the port is set to the authentication VLAN. After the client is authenticated and certified, the port is set to the access VLAN specified in the Port profile (Default Access VLAN, or User Role VLAN, or Initial Port VLAN).

In OOB Real-IP gateway mode, the CAM enables port bouncing to help clients acquire a new IP address after successful authentication and certification. In OOB Virtual Gateway mode, port bouncing is not necessary as the client uses the same IP address after successful authentication and certification.

Note If the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to "kick" the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see Configure Access to Authentication VLAN Change Detection, page 3-67.

Figure 3-17 Port Profiles List



Note The Policy Sync feature allows OOB Port Profiles and VLAN Profiles to be exported from a Master CAM to Receiver CAMs. Refer to Policy Import/Export, page 14-28 for details.

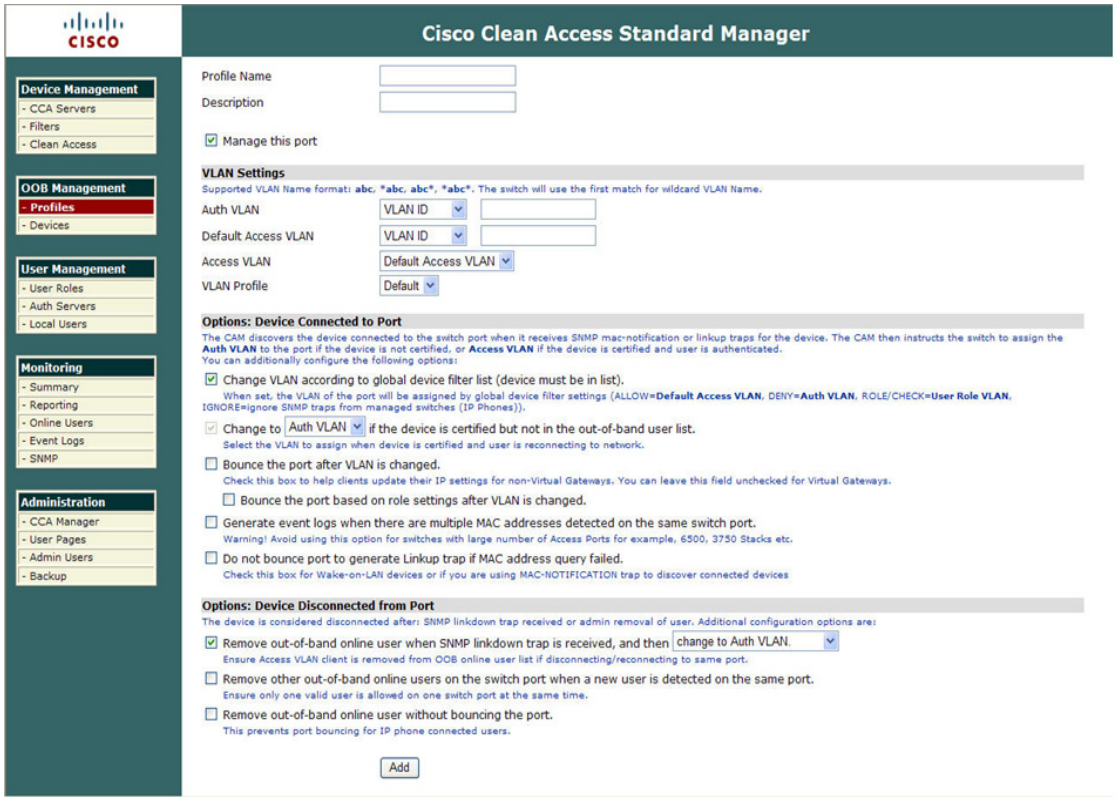
Add Port Profile

You will need to add a Port profile for each set of Authentication/Access VLANs you configure on the switch.

Note For OOB Virtual Gateways, you must enable and configure VLAN mapping on the CAS for each Authentication/Access VLAN pair configured on the switch. See Figure 3-8 on page 3-27 for more details.

Step 1 Go to **OOB Management > Profiles > Port > New** (Figure 3-18)

Figure 3-18 New Port Profile


Cisco Clean Access Standard Manager
Device Management
- CCA Servers
- Filters
- Clean Access
OOB Management
- Profiles
- Devices
User Management
- User Roles
- Auth Servers
- Local Users
Monitoring
- Summary
- Reporting
- Online Users
- Event Logs
- SNMP
Administration
- CCA Manager
- User Pages
- Admin Users
- Backup
Profile Name
Description
Manage this port
VLAN Settings
Supported VLAN Name format: abc, *abc, abc*, *abc*. The switch will use the first match for wildcard VLAN Name.
Auth VLAN
VLAN ID
Default Access VLAN
VLAN ID
Access VLAN
Default Access VLAN
VLAN Profile
Default
Options: Device Connected to Port
The CAM discovers the device connected to the switch port when it receives SNMP mac-notification or linkup traps for the device. The CAM then instructs the switch to assign the Auth VLAN to the port if the device is not certified, or Access VLAN if the device is certified and user is authenticated.
You can additionally configure the following options:
Change VLAN according to global device filter list (device must be in list).
When set, the VLAN of the port will be assigned by global device filter settings (ALLOW=Default Access VLAN, DENY=Auth VLAN, ROLE/CHECK=User Role VLAN, IGNORE=ignore SNMP traps from managed switches (IP Phones)).
Change to Auth VLAN if the device is certified but not in the out-of-band user list.
Select the VLAN to assign when device is certified and user is reconnecting to network.
Bounce the port after VLAN is changed.
Check this box to help clients update their IP settings for non-Virtual Gateways. You can leave this field unchecked for Virtual Gateways.
Bounce the port based on role settings after VLAN is changed.
Generate event logs when there are multiple MAC addresses detected on the same switch port.
Warning! Avoid using this option for switches with large number of Access Ports for example, 6500, 3750 Stacks etc.
Do not bounce port to generate Linkup trap if MAC address query failed.
Check this box for Wake-on-LAN devices or if you are using MAC-NOTIFICATION trap to discover connected devices
Options: Device Disconnected from Port
The device is considered disconnected after: SNMP linkdown trap received or admin removal of user. Additional configuration options are:
Remove out-of-band online user when SNMP linkdown trap is received, and then change to Auth VLAN.
Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnecting to same port.
Remove other out-of-band online users on the switch port when a new user is detected on the same port.
Ensure only one valid user is allowed on one switch port at the same time.
Remove out-of-band online user without bouncing the port.
This prevents port bouncing for IP phone connected users.
Add
360185

Step 2 Type a single word for the **Profile Name**. You can use digits and underscores, but no spaces. The name should reflect whether the Port profile is managed or unmanaged.

Note In addition to providing a Port Profile name that reflects whether the port to which this profile is applied is managed or unmanaged, Cisco recommends you also provide information about the nature of the port profile if the purpose is to ensure reliable client machine connection through a network IP phone.

Step 3 Type an optional **Description** for the Port profile.

Step 4 Click the checkbox for **Manage this port** to enable configuration of this Port profile. This enables the port management options on the page.

Step 5 For **Auth VLAN,** choose either **VLAN ID** (default) or **VLAN Name** from the dropdown menu and type the corresponding authentication/quarantine VLAN ID or name to be used for this port profile:

- If choosing **VLAN ID**—you can specify only numbers in the text field.
- If choosing **VLAN Name**—the text field is case-sensitive. You can specify wildcards for the VLAN name, such as: abc, *abc, abc*, or *abc*. The switch will use the first match for the wildcard VLAN name. You can also use special characters in the name.

Step 6 For **Default Access VLAN**, choose either **VLAN ID** (default) or **VLAN Name** from the dropdown and type the corresponding VLAN ID or name to be used as the default access VLAN for this port profile.

- If choosing **VLAN ID**—you can specify only numbers in the text field.
- If choosing **VLAN Name**—the text field is case-sensitive. You can specify wildcards for the VLAN name, such as: abc, *abc, abc*, or *abc*. The switch will use the first match for the wildcard VLAN name. You can also use special characters in the name.

Note If the switch cannot find the VLAN specified (e.g. the **VLAN Name** is mistyped), an error also appears on the perfigo.log (not the Event Log).

Step 7 For **Access VLAN**, choose one of the following options from the dropdown menu:

- **Default Access VLAN**—The CAM will put authenticated users with certified devices on the Default Access VLAN specified in the Port Profile.
- **User Role VLAN**—The CAM will put authenticated users with certified devices on the Access VLAN specified in the User Role (for details, see Figure 3-9: Configure User Role with Access VLAN and Out-of-Band User Role VLAN, page 6-10).
- **Initial Port VLAN**—The CAM will put authenticated users with certified devices on the **Initial VLAN** specified for the port in the **Ports** configuration page (see Ports Management Page, page 3-54 for details). The initial VLAN is the value saved by the CAM for the port when the switch is added. Instead of using a specified Access VLAN, the client is switched from the initial port VLAN to an Auth VLAN for authentication and certification, then switched back to the initial port VLAN when the client is certified.

Step 8 If you want to specify the Access VLAN using a VLAN profile definition, choose one of the **VLAN Profile** names you created in Add VLAN Profile, page 3-42 or choose **Default** from the dropdown menu to specify the VLAN profile to associate with this port profile.

Note If you choose Default, or if you have not yet created any custom VLAN profiles, the CAM queries only the managed switch in question for the VLAN name-to-VLAN ID mapping to determine the user's Access VLAN.

Port Profile Options when Device is Connected to Port

The CAM discovers the device connected to the switch port from SNMP MAC change notification/MAC move notification or linkup traps received. The port is assigned the **Auth VLAN** if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated. You can additionally configure the following options:

Step 9 Click the **Change VLAN according to global device filter list** option if you have configured a global Device Filter to ignore MAC addresses for IP phones in your network or if you want to use the CAM's global Device Filter rules to set the VLAN of the port. You must have device filters added under **Device Management > Filters > Devices** for this feature to work. For OOB, the device filter rules are as follows:

- **ALLOW**—bypass login and posture assessment (certification) and assign **Default Access VLAN** to the port
- **DENY**—bypass login and posture assessment (certification) and assign **Auth VLAN** to the port
- **ROLE**—bypass login and L2 posture assessment (certification) and assign **User Role VLAN** to the port (see Out-of-Band User Role VLAN, page 6-10)
- **CHECK**—bypass login, apply posture assessment, and assign **User Role VLAN** to the port (see Out-of-Band User Role VLAN, page 6-10)
- **IGNORE**—ignore SNMP traps from managed switches (IP Phones)

Note Cisco recommends enabling this option for all Out-of-Band deployments to ensure the most accurate status updates in the Out-of-Band Online Users list, and ensure that you do not configure any local (CAS-based) device filters that would potentially conflict with this global setting.

Rules configured for MAC addresses on the global Device Filter list have the highest priority for user/device processing in both OOB and IB deployments. See Device Filters for Out-of-Band Deployment, page 2-14 for further details.

For more information on In-Band vs. Out-of-Band client machine behavior based on specified Device Filter type, see In-Band and Out-of-Band Device Filter Behavior Comparison, page 2-16.

Step 10 The **Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the Out-of-Band user list** option is automatically enabled when a port is managed. Choose which VLAN to use when the device is certified and the user is reconnecting to the port:

- **Default Auth VLAN**—Force Access VLAN clients on this port to re-authenticate on the Authentication VLAN the next time they connect to the network.
- **Default Access VLAN**—Allow clients to stay on the trusted network without having to login again the next time they connect to the network.

Step 11 Use the **Bounce the port after VLAN is changed** option to specify port behavior following VLAN change:

- For Real-IP gateways, check this box to prompt the client to get a new IP address once switched to the Access VLAN.
- For Virtual gateways, leave this box unchecked.

Note If using a version 4.1.2.0 or later Windows Agent, ActiveX Control, or Java Applet to refresh client DHCP IP addresses, the **Bounce the switch port after VLAN is changed** option in the Port profile can be left disabled. Refer to DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6, Configure Access to Authentication VLAN Change Detection, page 3-67, and see Advanced Settings, page 3-45 for additional details on configuring DHCP Release, VLAN Change, and DHCP Renew delays.

Step 12 When you enable the **Bounce the port based on role settings after VLAN is changed** option, the switch defers to the associated user role to determine port bouncing and/or IP address refresh/renew behavior when the VLAN of the port through which the user is accessing the network switches from the authentication to the access VLAN. Both of the user role options are on the **User Management > User Roles > New Role** page.

Note If you enable the **Bounce the port after VLAN is changed** option in step 11 above, this option is inaccessible.

Step 13 You can check the **Generate event logs when there are multiple MAC addresses detected on the same switch port** box to generate event logs when multiple MAC addresses are found on the same switch port.

Warning **Avoid using this option for switches with large number of Access Ports such as 6500 and 3750 stacks.**

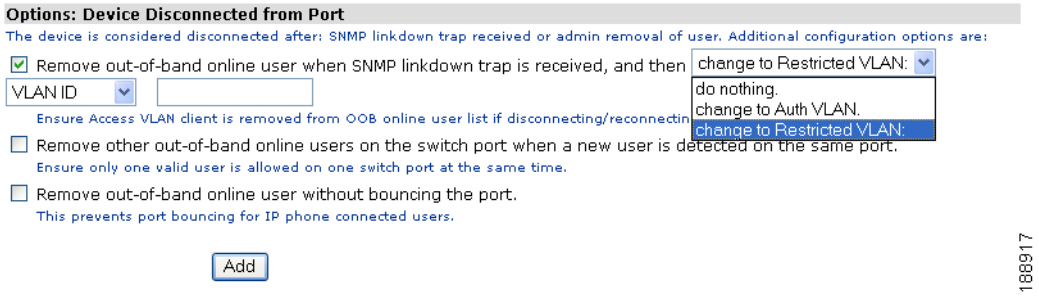
Step 14 You can enable the **Do not bounce port to generate Linkup trap if MAC address query failed** checkbox to wake up LAN devices or when you are using MAC-NOTIFICATION trap to discover connected devices.

Port Profile Options when Device is Disconnected from Port

A device is considered disconnected after one of the following events occurs:

- User disconnects from network and CAM receives SNMP linkdown trap
- Administrator removes user from OOB users list

Figure 3-19 Options: Device Disconnected from Port


Options: Device Disconnected from Port
The device is considered disconnected after: SNMP linkdown trap received or admin removal of user. Additional configuration options are:
Remove out-of-band online user when SNMP linkdown trap is received, and then
change to Restricted VLAN:
do nothing.
change to Auth VLAN.
change to Restricted VLAN:
VLAN ID
Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnectin
Remove other out-of-band online users on the switch port when a new user is detected on the same port.
Ensure only one valid user is allowed on one switch port at the same time.
Remove out-of-band online user without bouncing the port.
This prevents port bouncing for IP phone connected users.
Add
188917

Step 15 To remove OOB users from the Out-of-Band Online Users list and determine VLAN assignments for switch ports where client machines have disconnected from the network, you can configure the following options:

- **Remove Out-of-Band online user when SNMP linkdown trap is received, and then [do nothing | change to Auth VLAN | change to Restricted VLAN]**

  Click this option to specify which VLAN the CAM assigns to a switch port after receiving a linkdown trap from the switch when a client disconnects from the Cisco NAC Appliance network. (See Advanced, page 3-64 for details on linkdown traps.)

  - If this option is checked and specifies to **do nothing**, when the client disconnects (causing a linkdown trap to be sent), the switch port remains on the last VLAN assigned, or re-assigned to the VLAN specified in the **Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the Out-of-Band user list** option.

    Note If the client is not on the Certified Devices List, the client is put on the Authentication VLAN.

  - If this option is checked and specifies to **change to Auth VLAN**, the CAM puts the switch port on the Authentication VLAN after receiving a linkdown SNMP trap regardless of whether or not the client is on the Certified Devices List.
  - If this option is checked and specifies to **change to Restricted VLAN**, the CAM either assigns the switch port to a previously-configured **VLAN Name** (see Configure VLAN Profiles, page 3-40 for more details), or to a specific **VLAN ID** number you enter in the text field that appears under this setting. As with the **change to Auth VLAN** option, this VLAN assignment takes place when the CAM receives a linkdown trap regardless of whether or not the client is on the Certified Devices List.

- **Remove other Out-of-Band online users on the switch port when a new user is detected on the same port**

This feature enables administrators to remove other online Out-of-Band users on the switch port when a new user is detected on the same port. It also allows for the modification of the port profile if an existing user is seen on a different switchport.

Checking this option ensures that only one valid user is allowed on one switch port at the same time. If an online user (e.g."user1") is currently on a switch port (e.g. "fa0/1" on switch "c2950") and this option is enabled for the Port Profile applied to that port, "user1" will be removed if another user (e.g "user2") signs in from the same switch port or moves to this port from another location.



Note Online user is an endpoint or a PC connected to the switch port. If another user logs in to the same PC with different credentials, it is not detected as a different user, as the endpoint is identified only by the MAC Address and not by the login credentials.

- **Remove Out-of-Band online user without bouncing the port**

  When any user is removed from the OOB Online User list, the port is changed from the Access VLAN to the Authentication VLAN. Also note that users removed from the Certified Device list are also always removed from the Online User list (IB or OOB). If the **Remove Out-of-Band online user without bouncing the port** option is checked, the port will not be bounced when a user is removed from the OOB Online User list. If this option is not checked, the port will be bounced when a user is removed from the OOB Online User list.

  This option is intended to prevent bouncing the switch port to which a client machine is connected via an IP phone. The feature allows Cisco NAC Appliance to authenticate/assess/quarantine/remediate a client machine (laptop/desktop) without affecting the operation of a IP phone connected to the switch port. When this option is checked for OOB Virtual Gateways, the client port will not be bounced when:

  – Users are removed from the Out-of-Band Online Users list
  – Devices are removed from the Certified Devices List

  Instead, the port Access VLAN will be changed to the Authentication VLAN.

Step 16 Click **Add** to add the port profile to the **OOB Management > Profiles > Port > List**.

See Manage Switch Ports, page 3-54 for further details on Port profiles and the **Ports** config page.

See Interpreting Event Logs, page 13-4 for further details on monitoring online users.

Configure VLAN Profiles

You can use VLAN profiles on your Cisco NAC Appliance to resolve VLAN name-to-VLAN ID mappings while simultaneously ensuring uniform L3 OOB support for multiple access points on your network. VLAN profiles work in conjunction with port profiles to specify the Access VLAN for a user session based on a set of VLAN name-to-VLAN ID mappings. If you have a single access point for remote users on your network, VLAN profiles likely serve very little purpose. If, however, your network includes two, three, or even dozens of different access points, VLAN profiles can help you dynamically assign Access VLAN IDs for remote users based on a "user friendly" VLAN name assignment associated with the user's profile configured on the system.

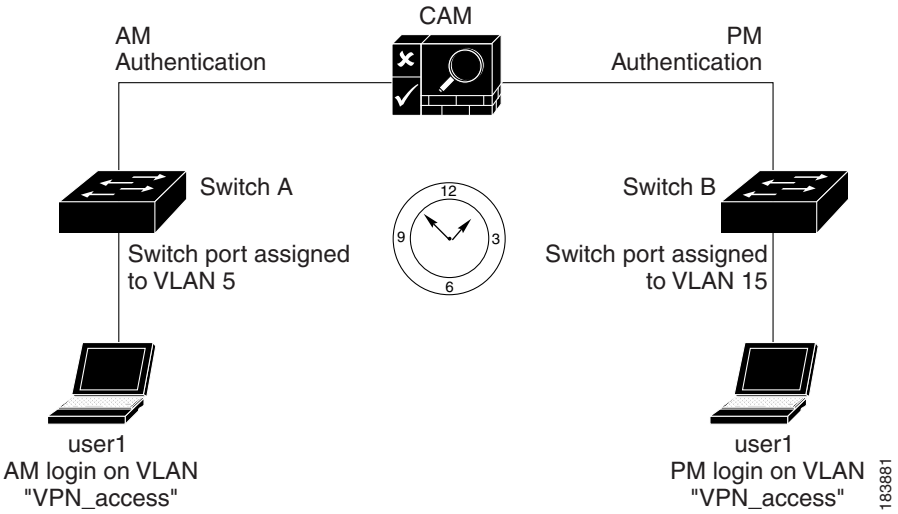
When a remote user accesses the network for authentication, the Cisco NAC Appliance assigns the user session to an Authentication VLAN before granting network access. Once the user is authenticated, the CAM instructs the access switch (the switch through which the user is accessing the network) to assign a VLAN ID to the managed port, based on Default Access VLAN, User Role VLAN, or Initial Port VLAN definitions.

There are two methods to determine VLAN name-to-VLAN ID mapping criteria:

- Querying local (CAM) VLAN profiles
- Querying the VLAN name-to-VLAN ID maps on the access switch, itself

You can configure the CAM to query only the local database, only the switch database, or both sources in the order you specify. When a user logs in to the network from a given access point and has been authenticated, they may be assigned one VLAN ID for one switch and a different VLAN ID for another. Figure 3-20 provides an example of this feature in a remote-access scenario.

Figure 3-20 VLAN Profile Feature Example



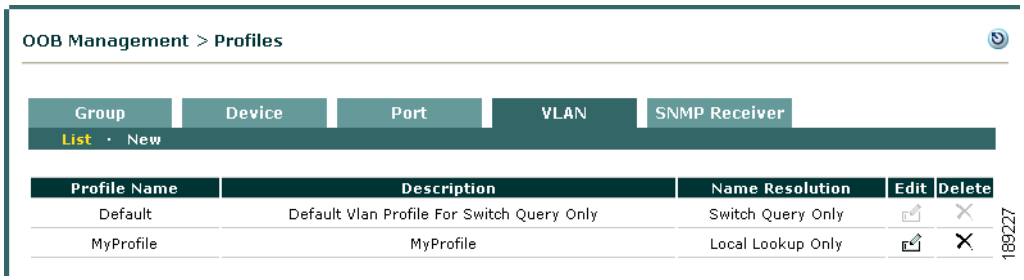
1. In the morning, user1 attempts to remotely access the network and his session arrives via switch A. Switch A allows the user authentication-level access and user1 passes authentication credentials on to the CAM.
2. Upon receiving the authentication request, the CAM discovers the Access VLAN for user1's session is defined in the associated user role, which specifies a VLAN name "VPN_access."
3. The CAM queries VLAN profile assignments for the VLAN ID corresponding to "VPN_access" and discovers a VLAN profile associated with the port profile for Switch A indicating VLAN 5.

4. User1 is authenticated and the CAM instructs switch A to assign VLAN 5 to the managed port.
5. User1 achieves VPN access to the internal network.
6. Later in the day, while visiting a client, user1 again attempts to access the network, but this time user1's session arrives at access switch B.
7. As with switch A earlier that day, switch B allows the user authentication-level access and user1 passes authentication credentials on to the CAM, where the same user role association specifies that the Access VLAN for user1's session should be the VLAN name "VPN_access."
8. The CAM queries VLAN profile assignments for the VLAN ID corresponding to "VPN_access" and, because switch B employs a different VLAN ID assignment model addressed in the relevant CAM switch profile mappings, the CAM discovers a VLAN profile associated with the port profile for Switch B indicating VLAN 15.
9. The CAM instructs switch B to assign VLAN 15 to the managed switch port and grant VPN access to user1.

As this example demonstrates, the VLAN access name is the same for both sessions, but two separate VLAN profiles on the CAM ensure user1 receives the same level of authentication from both access points on the network.

Figure 3-21 illustrates the VLAN Profiles List page.

Figure 3-21 VLAN Profiles



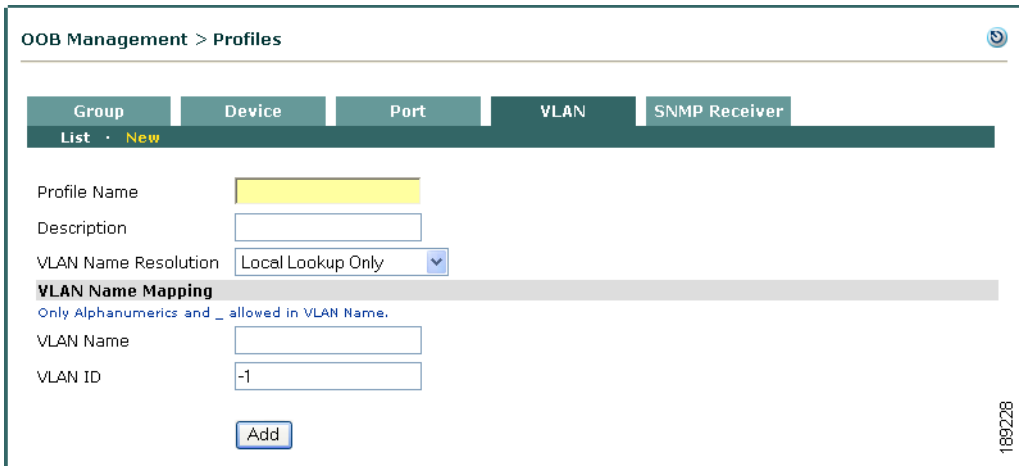
Note The Policy Sync feature allows OOB Port Profiles and VLAN Profiles to be exported from a Master CAM to Receiver CAMs. Refer to Policy Import/Export, page 14-28 for details.

Add VLAN Profile

To create a new VLAN profile:

Step 1 Go to **OOB Management > Profiles > VLAN > New** (Figure 3-22).

Figure 3-22 New VLAN Profile



Step 2 Specify a unique **Profile Name** for the new VLAN profile.

Step 3 Type an optional **Description** for the VLAN profile.

Step 4 Choose a **VLAN Name Resolution** method from the dropdown list:

- **Local Lookup Only**—Instructs the CAM to resolve the specified VLAN name using only local mappings as the possible resolved values. If you select this option, the CAM will not attempt to resolve the VLAN name using any data available on the access switch.
- **Switch Query Preferred**—Instructs the CAM to resolve the specified VLAN name by first searching data available from the access switch, *then* (if not found) attempting to resolve the name in the VLAN Name-to-ID mappings found in the VLAN profile.
- **Local Lookup Preferred**—Instructs the CAM to resolve the specified VLAN name by first searching name in the VLAN Name-to-ID mappings found in the VLAN profile, *then* (if not found) attempting to resolve the name by searching data available from the access switch.

Step 5 Enter the **VLAN Name** for the access VLAN (the assigned "common" name of the VLAN users can access the network) the CAM uses to grant access to the remote user. This function allows you to use VLAN names instead of specific VLAN numbers to identify the VLAN ID the CAM should instruct the access switch(es) to assign to the port over which the user accesses the network. Since the user may access the network from one of several access switches residing at different network access points, the VLAN name-to-VLAN ID mapping function enables you to associate a specific VLAN name with a user or group profile and grant access over a broad range of access devices all around the network, based on a single VLAN profile definition.

Step 6 Enter the **VLAN ID** for the VLAN policy. This is the actual VLAN number the CAS tells the switch to assign to the remote user's switch port once the user logs in and has been "cleared" to access the internal network. Because VLAN IDs from different switches may be (and probably are) different, you can grant access to a user or group profile based on the VLAN name-to-VLAD ID mapping defined on the CAM and/or the access switch, itself.

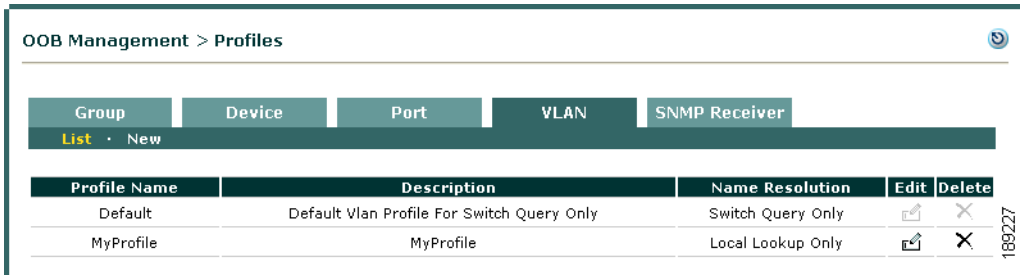
Step 7 Click **Add**.

Edit VLAN Profile

To edit an existing VLAN profile:

Step 1 Go to **OOB Management > Profiles > VLAN > List** (Figure 3-23).

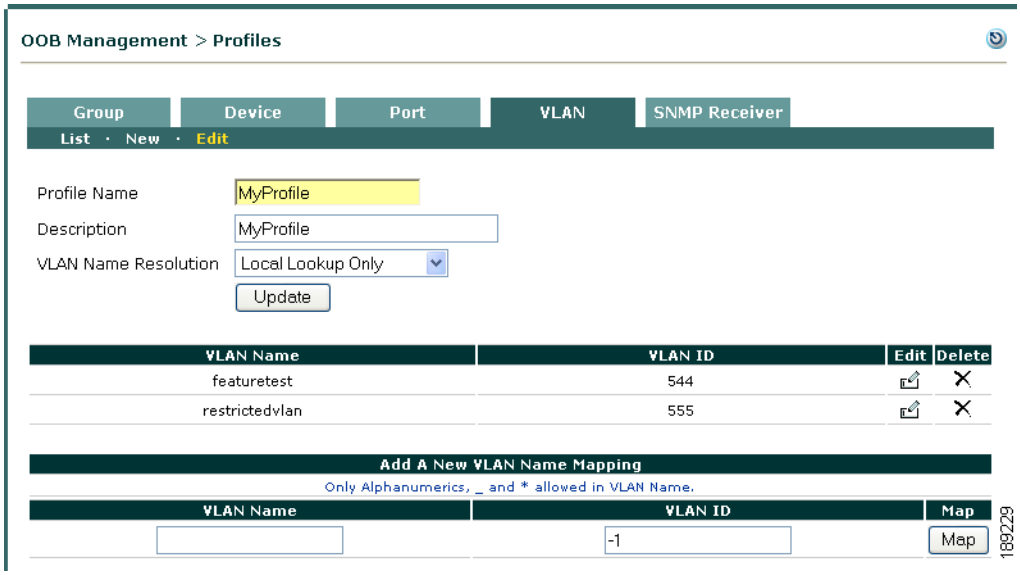
Figure 3-23 VLAN Profiles



Step 2 Click the **Edit** icon for the existing VLAN profile you want to update.

The Edit VLAN Profile window (Figure 3-24) appears.

Figure 3-24 Edit VLAN Profile



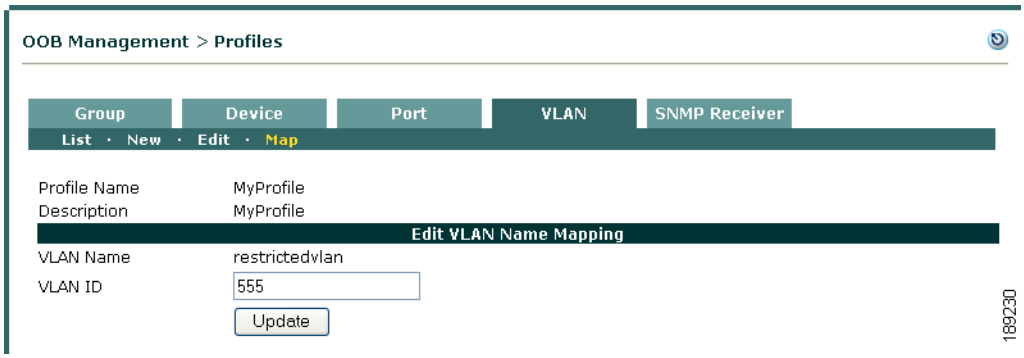
Step 3 Enter a new **Profile Name**, **Description**, and/or specify a different **VLAN Name Resolution** lookup method for the VLAN profile and click **Update**.

Step 4 To update VLAN name-to-VLAN ID mappings:

a. If you want to add a new VLAN name-to-VLAN ID mapping, specify the additional **VLAN Name** and **VLAN ID** under Add a New VLAN Name Mapping and click **Map**.

b. If you want to reassign one or more VLAN name-to-VLAN ID mappings, click the **Edit** icon corresponding to the mapping you want to update, specify a new **VLAN ID** under Edit VLAN Name Mapping, and click **Update**. (See Figure 3-25.)

Figure 3-25 Edit VLAN Name Mapping—VLAN ID



Configure SNMP Receiver

The **SNMP Receiver** form configures how the SNMP Receiver running on the Clean Access Manager receives and responds to SNMP trap notifications from all managed switches when MAC change notification/MAC move notification or linkup/linkdown user events occur (such as when a user plugs into the network). The configuration on the switch must match the CAM's SNMP Receiver configuration in order for the switch to send traps to the CAM.

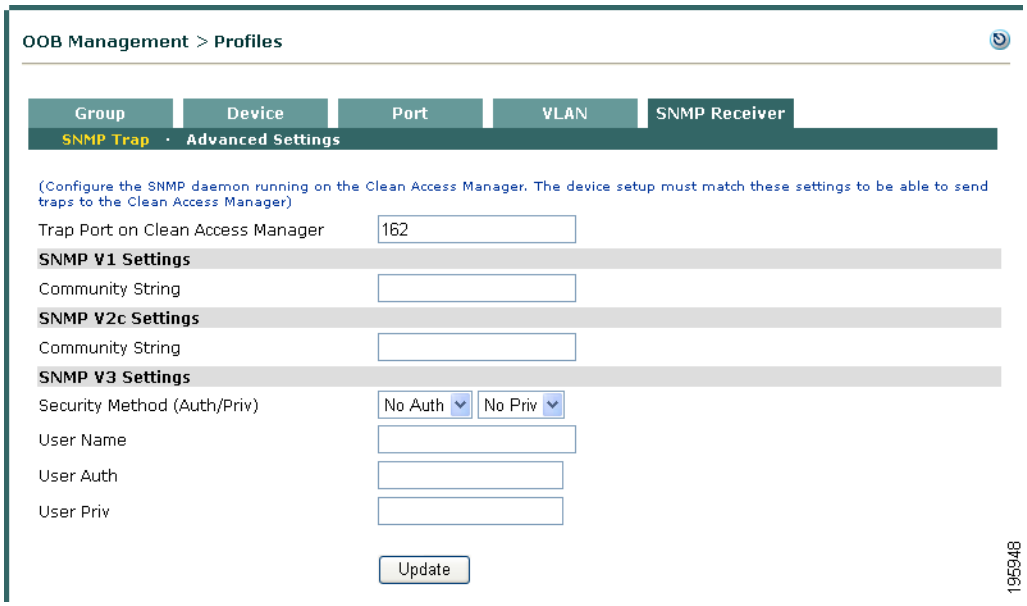
Cisco NAC Appliance also provides support for SHA-1 and 3DES encryption, which is required when configuring SNMP management on a CAM operating in a FIPS 140-2 compliant network.

SNMP Trap

This page configures settings for the SNMP traps the CAM receives from all switches. The Clean Access Manager SNMP Receiver can support simultaneous use of different versions of SNMP (V1, V2c, V3) when controlling groups of switches in which individual switches may be using different versions of SNMP.

Step 1 Go to **OOB Management > Profiles > SNMP Receiver > SNMP Trap** (Figure 3-26).

Figure 3-26 CAM SNMP Receiver



Step 2 Use the default **Trap Port on Clean Access Manager** (162) or enter a new port number here.

Step 3 For **SNMP V1 Settings**, type the **Community String** used on switches using SNMP V1.

Step 4 For **SNMP V2c Settings**, type the **Community String** used on switches using SNMP V2c.

Step 5 For **SNMP V3 Settings**, configure the following fields used on switches using SNMP V3:

- Specify the SNMP V3 authentication and privacy combination using the **Security Method (Auth/Priv)** dropdown menus:
  - NoAuth, MD5 (non-FIPS only), SHA-1
  - NoPriv, DES (non-FIPS only), 3DES

Note If you are specifying an authentication/privacy combination for a FIPS 140-2 compliant CAM, the only settings available are the SHA-1 authentication and 3DES privacy types.

- Type the **User Name**.
- Type the **User Auth.**
- Type the **User Priv**

Step 6 Click **Update** to save settings.

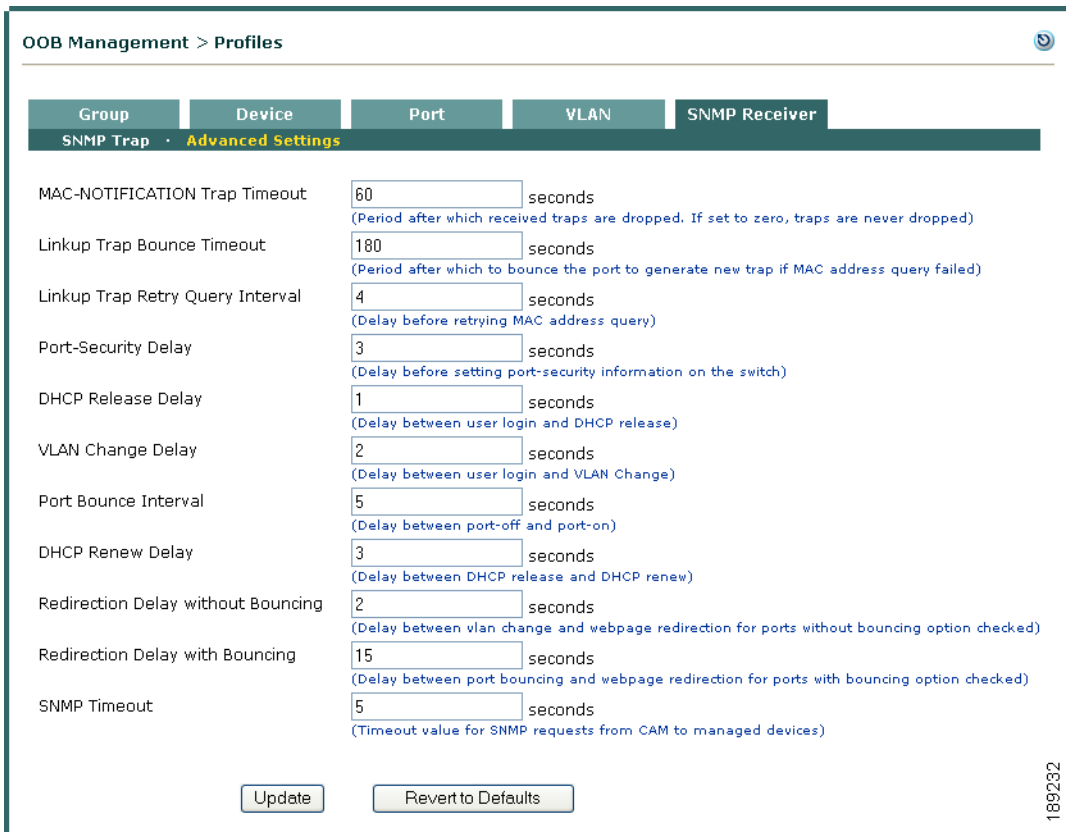
Advanced Settings

This page configures advanced timeout and delay settings for the SNMP traps received and sent by the Clean Access Manager (CAM). To change the default settings, use the following steps. You can use the page to fine-tune settings from their defaults once switches are added and configured.

To Change Default SNMP

Step 1 Go to **OOB Management > Profiles > SNMP Receiver > Advanced Settings** (Figure 3-27).

Figure 3-27 SNMP Receiver > Advanced Settings


OOB Management > Profiles
Group
Device
Port
VLAN
SNMP Receiver
SNMP Trap · Advanced Settings
MAC-NOTIFICATION Trap Timeout
60 seconds
(Period after which received traps are dropped. If set to zero, traps are never dropped)
Linkup Trap Bounce Timeout
180 seconds
(Period after which to bounce the port to generate new trap if MAC address query failed)
Linkup Trap Retry Query Interval
4 seconds
(Delay before retrying MAC address query)
Port-Security Delay
3 seconds
(Delay before setting port-security information on the switch)
DHCP Release Delay
1 seconds
(Delay between user login and DHCP release)
VLAN Change Delay
2 seconds
(Delay between user login and VLAN Change)
Port Bounce Interval
5 seconds
(Delay between port-off and port-on)
DHCP Renew Delay
3 seconds
(Delay between DHCP release and DHCP renew)
Redirection Delay without Bouncing
2 seconds
(Delay between vlan change and webpage redirection for ports without bouncing option checked)
Redirection Delay with Bouncing
15 seconds
(Delay between port bouncing and webpage redirection for ports with bouncing option checked)
SNMP Timeout
5 seconds
(Timeout value for SNMP requests from CAM to managed devices)
Update
Revert to Defaults
189232

Step 2 Configure optional Advanced Settings as follows:

- **MAC-NOTIFICATION Trap Timeout** (default is 60 seconds)—The CAM timestamps the MAC change notification/MAC move notification traps it receives, and examines the timestamp when the trap is processed. If the time difference between the timestamp and the current time is greater than the **MAC-NOTIFICATION Trap Timeout**, the trap is dropped. This configuration fields ensures the CAM only processes timely traps.
- **Linkup Trap Bounce Timeout** (default is 180 seconds)—When the CAM receives a linkup trap, it tries to resolve the MAC address connected to the port. The MAC address may not be available at that time. If the CAM cannot get the MAC address, it makes another attempt after the number of seconds specified in the **Linkup Trap Retry Query Interval** field. In order to keep the port controlled and limit the number of times the CAM tries to resolve the MAC address, the CAM bounces the port after the number of seconds specified in the **Linkup Trap Bounce Timeout** to force the switch to generate a new linkup trap.
- **Linkup Trap Retry Query Interval** (default is 4 seconds)—When the CAM receives a linkup trap, it needs to query the switch for the MAC address connected to the port. If the MAC address is not yet available, the CAM waits the number of seconds specified in the **Linkup Trap Retry Query Interval** field, then tries again.

- **Port-Security Delay** (default is 3 seconds)—If port-security is enabled on the switch, after the VLAN is switched, the CAM must wait the number of seconds specified in the **Port-Security Delay** field before setting the port-security information on the switch.

Note To refresh the DHCP IP address, typically the Agent or ActiveX/Java Applet performs a DHCP release before the VLAN change, followed by a DHCP renew after the VLAN change. The delays to perform DHCP Release, VLAN Change, DHCP Renew are configurable. See DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6 for additional details. See also Configure Access to Authentication VLAN Change Detection, page 3-67 if you are using DHCP release/renew instead of port bouncing.

- **DHCP Release Delay** (default is 1 second)—This field configures the delay between user login and DHCP release.
- **VLAN Change Delay** (default is 2 seconds)—This field configures the delay between user login and VLAN Change. This value should be greater than the **DHCP Release Delay**.

Note The **VLAN Change Delay** setting should be greater than the **DHCP Release Delay**, but less than the combined duration of the **DHCP Release Delay** and **DHCP Renew Delay**. This is to ensure that DHCP release happens before VLAN change and DHCP renew happens after VLAN change.

- **Port Bounce Interval** (default is 5 seconds)—The **Port Bounce Interval** is the time delay between turning off and turning on the port. This delay is inserted to help client machines issue DHCP requests.
- **DHCP Renew Delay** (default is 3 seconds)—This field configures the delay between DHCP release and DHCP renew. This value should be greater than the **VLAN Change Delay** minus the **DHCP Release Delay**.
- **Redirection Delay without Bouncing** (default is 1 second)—This field configures the delay between VLAN change and webpage redirection (after client posture assessment) for ports with no port bouncing in the Port Profile. This allows you to minimize redirection time if no port bouncing is required. When the Port Profile does not require bouncing the port after the VLAN is changed (e.g Virtual Gateway), configuring this option will redirect the user page after the number of seconds specified here (e.g. 1 second).

  When the port is not bounced, the total redirection interval that the user experiences is the value of the **Redirection Delay without Bouncing** field.

Note When the user continues to be redirected to the login page after login/posture assessment, this typically means the web page redirection is occurring before the switch is able to change the VLAN of the port (from Auth to Access). In this case, increase the Redirection Delay to 2 or 3 seconds to resolve this issue.

- **Redirection Delay with Bouncing** (default is 15 seconds)—This field configures the delay between port bouncing and webpage redirection (after client posture assessment) for ports with the **Bounce the port after VLAN is changed** option checked on the Port Profile. This allows you to configure the time needed for port bouncing.

  When the port is bounced, the total redirection interval that the user experiences is the sum of 2 fields: **Redirection Delay with Bouncing** and **Port Bounce Interval**.

If the Port Profile requires bouncing the port after the VLAN is changed, then after user login, the user will see “Renewing IP address” page after the sum of the number of seconds specified in this field and the number of seconds specified in the **Port Bounce Interval**. For example:

Port Bounce (5 seconds) + Redirection Delay (15 seconds) = Redirection interval (20 seconds total)

- **SNMP Timeout** (default is 5 seconds)—This field enables you to specify the SNMP timeout value (in seconds) for read/write requests, SNMP trap message responses from a managed switch that saves its current (running) configuration when instructed by the Clean Access Manager.

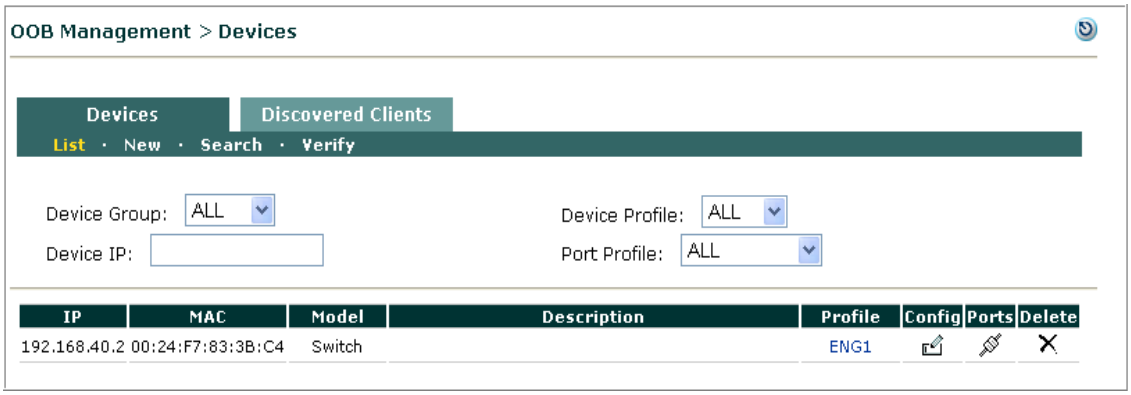
Step 3 Click **Update** to save settings.

Add and Manage Switches

The pages under the **OOB Management > Devices > Devices** tab are used to discover and add new managed switches within an IP range, add new managed switches by exact IP address, manage the list of controlled switches, and verify the switches and WLC.

- Add New Switch, page 3-49
- Search New Switches, page 3-50
- Verify Devices, page 3-51

Figure 3-28 List of Switches



The list of switches under **OOB Management > Devices > Devices > List** displays all switches and WLCs added from the **New** or **Search** forms. Switch entries in the list include the switch’s IP address, MAC address, Description, and Switch Profile. You can sort the entries on the list by **Device Group**, **Device Profile**, or **Port Profile** dropdowns, or you can simply type a **Device IP** and hit Enter to search for a switch or WLC by its address. Additionally the List provides one control and three icons:

- **Profile**—Clicking the **Profile** link brings up the Switch Profile (Figure 3-15).
- **Config**—Clicking the **Config** icon brings up the Config Tab, page 3-63 for the switch.
- **Ports**—Clicking the **Ports** icon brings up the Ports Management Page, page 3-54 for the switch.

Note WLC device profiles do not use Port Profile configurations. Therefore, the **Ports** icon remains “grayed out” for any WLC entries in the table.

- **Delete**—Clicking the **Delete** icon deletes the switch from the list (a confirmation dialog will appear first).

Note When adding a switch based on its loopback address, the **OOB Management > Devices > Devices > List** will display a MAC address of 00:00:00:00:00:00 for the switch. This is expected behavior; the MAC address displayed on this interface is for information only and does affect OOB functionality.

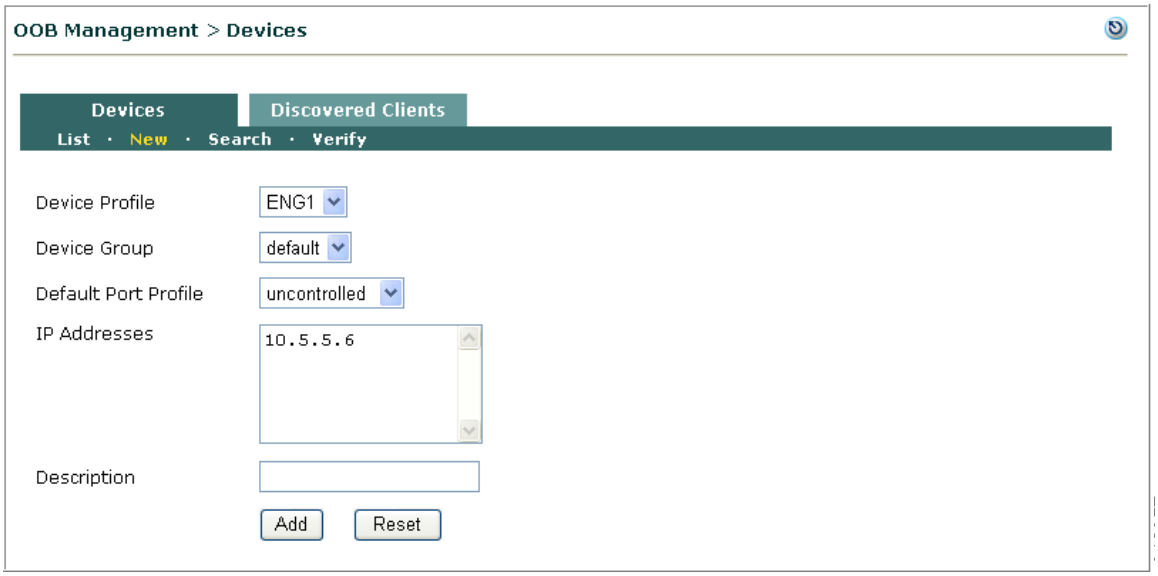
Add New Switch

The **New** page allows you to add switches when exact IP addresses are already known.

Note Cisco does not support third party devices. If a non-Cisco or a custom device (third party device) is added to NAC, then a message is displayed that the device being added is a non-Cisco device and support for non-Cisco devices is not guaranteed.

Step 1 Go to **OOB Management > Devices > Devices > New** (Figure 3-29).

Figure 3-29 Add New Switch



Step 2 Choose the **Device Profile** from the dropdown menu to apply to the switches or WLCs to be added.

Step 3 Choose the **Device Group** for the switches or WLCs from the dropdown menu.

Step 4 Choose the **Default Port Profile** from the dropdown menu. Typically, the default port profile should be uncontrolled.

Step 5 Type the **IP Addresses** of the switch(es) you want to add. Separate each IP address by line.

Step 6 Enter an optional **Description** of the new switch.

Step 7 Click the **Add** button to add the switch or WLC.

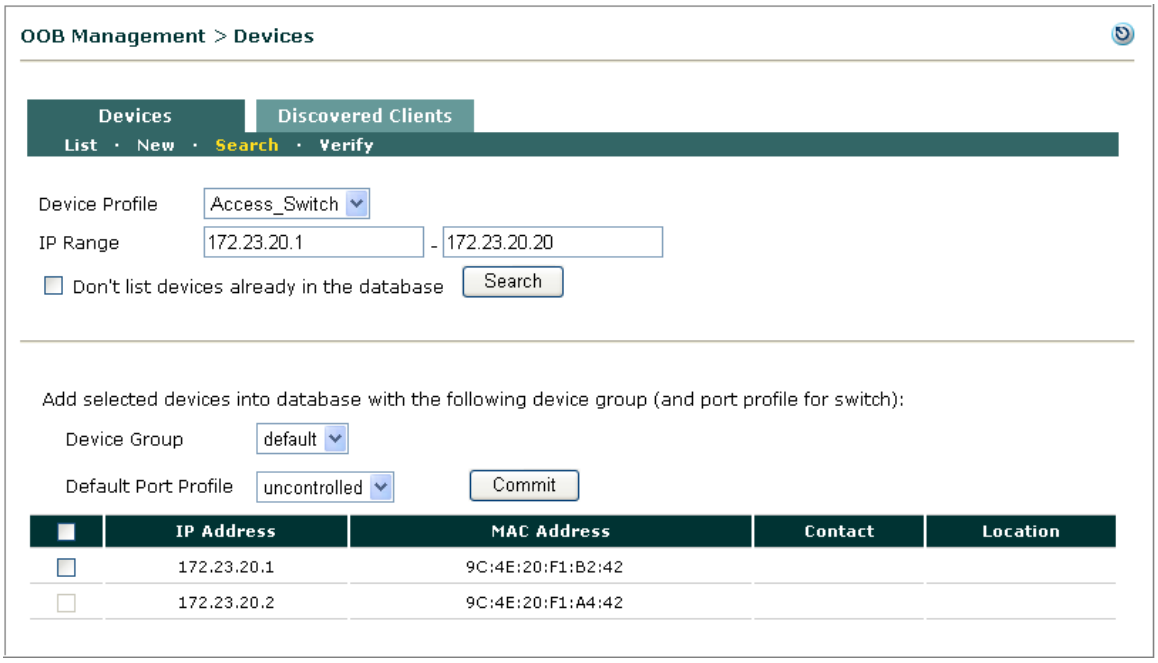
Step 8 Click the **Reset** button to reset the form.

Search New Switches

The **Search** page allows you to discover and add unmanaged switches within an IP range.

Step 1 Go to **OOB Management > Devices > Devices > Search** (Figure 3-30).

Figure 3-30 Search Switches



Step 2 Select a **Device Profile** from the dropdown list. The read community string of the selected Device Profile is used to find switches with matching read settings.

Step 3 Type an **IP Range** in the text box. Note that the maximum IP range is 256 for a search.

Step 4 By default, the **Don't list devices already in the database** checkbox is already checked. If you uncheck this box, the resulting search will include switches and WLCs you have already added. Note, however, that the Commit checkboxes to the left of each entry will be disabled for switches that are already managed.

Step 5 Choose a **Device Group** from the dropdown to apply to the unmanaged devices found in the search.

Step 6 Choose a **Default Port Profile** from the dropdown to apply to the unmanaged devices found in the search.

Step 7 Click the **checkbox** to the left of each unmanaged device you want to manage through the CAM. Alternatively, click the checkbox at the top of the column to add *all* unmanaged devices found from the search.

Note While all switches matching the read community string of the Switch Profile used for the search are listed, only those switches matching the *read* SNMP version and community string can be added using the **Commit** button. A switch cannot be controlled unless its *write* SNMP settings match those configured for its Switch Profile in the Clean Access Manager.

Step 8 Click the **Commit** button to add the new switches. These switches are listed under **OOB Management > Devices > Devices > List**.

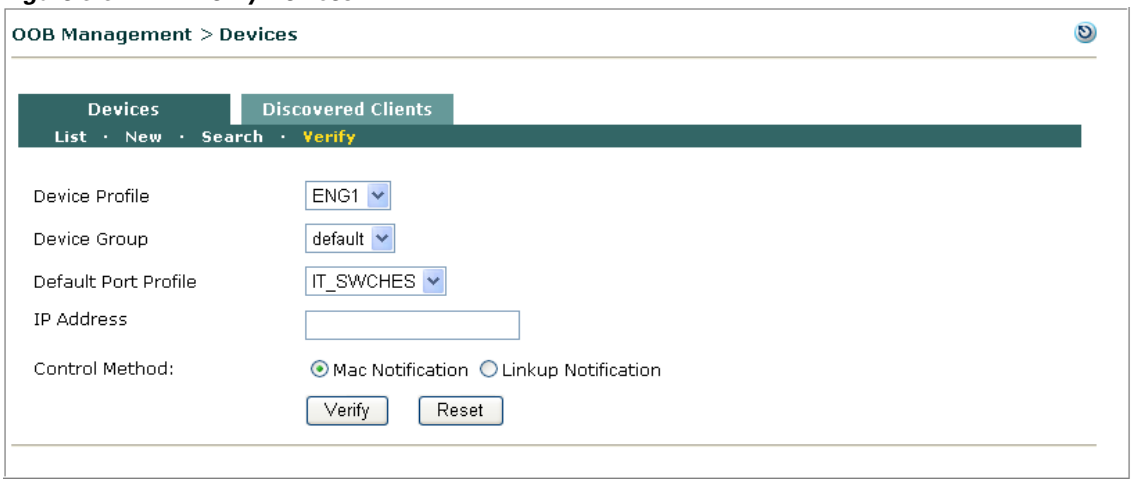
Verify Devices

The **Verify** page allows you to verify the devices. This utility verifies a device already added to CAM or a new device that is yet to be added to CAM. The device may be a switch or WLC.

Note Before verifying a device, ensure that you have setup the device profile and port profile, and configured the SNMP receiver for the device.

Step 1 Go to **OOB Management > Devices > Devices > Verify**.

Figure 3-31 Verify Devices



Step 2 Choose a **Device Profile** from the dropdown.

Step 3 Choose a **Device Group** from the dropdown.

Step 4 Choose a **Default Port Profile** from the dropdown.

Step 5 Type a valid **IP Address** in the text box.

Step 6 Choose the **Control Method** to configure the SNMP trap notification type that the CAM SNMP Receiver will use for a particular switch.

Note The **Control Method** is applicable only for the switches.

- **MAC Notification**—If a switch supports MAC Notification, choose this option.

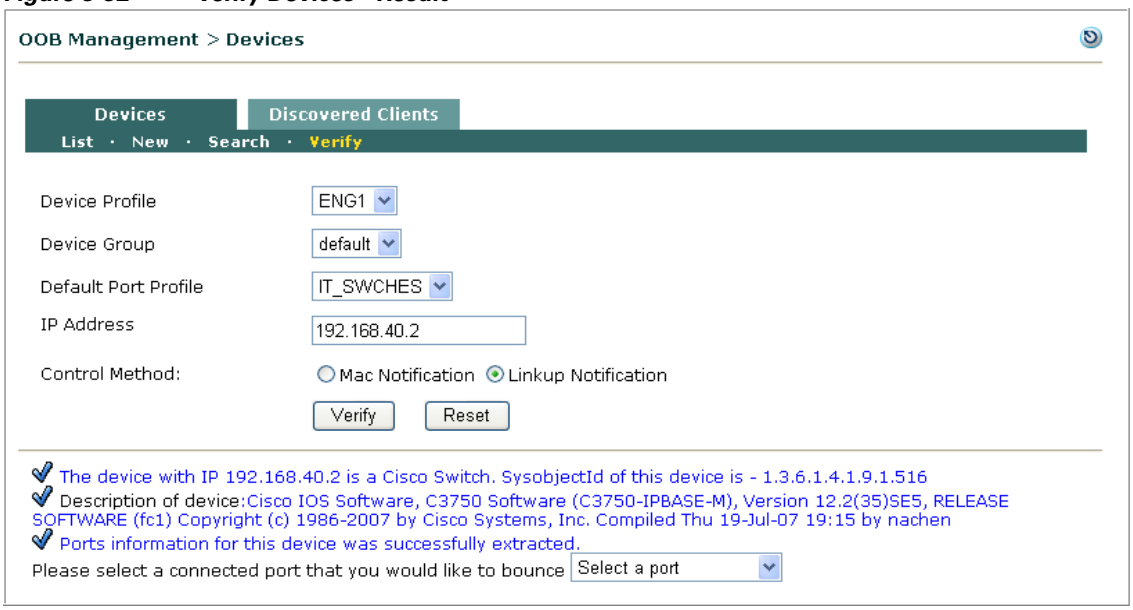
Note To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- **Linkup Notification**—If a switch does not support MAC Notification, then choose this option.

Step 7 Click **Verify**.

The device is verified and the results are displayed at the bottom of the page as shown in Figure 3-32.

Figure 3-32 Verify Devices - Result


OOB Management > Devices
Devices
Discovered Clients
List · New · Search · Verify
Device Profile
ENG1
Device Group
default
Default Port Profile
IT_SWCHES
IP Address
192.168.40.2
Control Method:
Mac Notification
Linkup Notification
Verify
Reset
The device with IP 192.168.40.2 is a Cisco Switch. SysobjectId of this device is - 1.3.6.1.4.1.9.1.516
Description of device:Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Thu 19-Jul-07 19:15 by nachen
Ports information for this device was successfully extracted.
Please select a connected port that you would like to bounce
Select a port
246960

The device status is displayed and you can select a connected port that you would like to bounce from the dropdown.

Discovered Clients

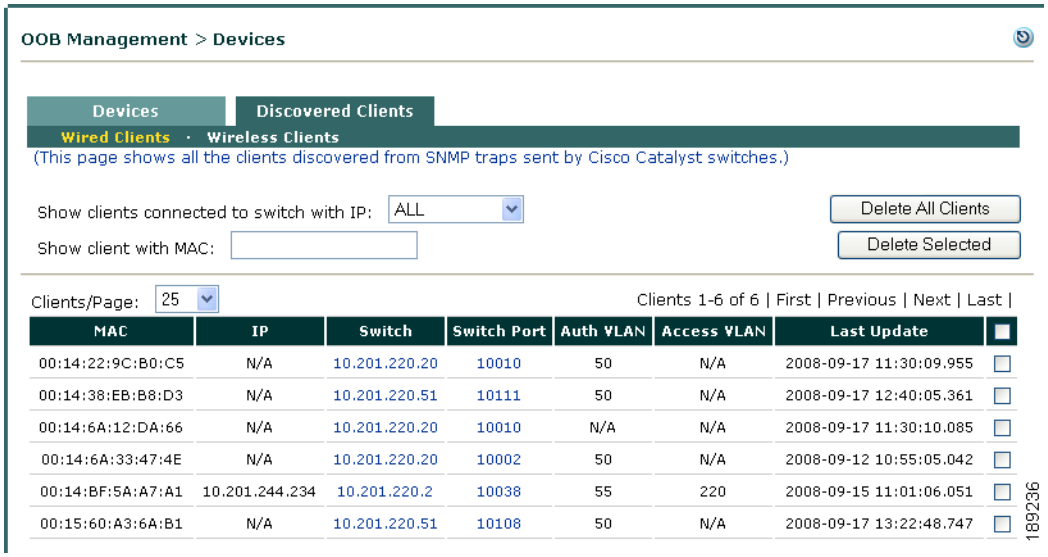
Figure 3-33 shows the **OOB Management > Devices > Discovered Clients > Wired Clients** page. The Wired Clients page lists all clients discovered by the Clean Access Manager via SNMP MAC change notification/MAC move notification and linkup/linkdown traps. The page records the activities of Out-of-Band clients (regardless of VLAN), based on the SNMP trap information that the Clean Access Manager receives.

When a client connects to a port on the Auth VLAN, a trap is sent and the Clean Access Manager creates an entry on the Wired Clients page. The Clean Access Manager adds a client's MAC address, originating switch IP address, and switch port number to the Out-of-Band Discovered Clients list. Thereafter, the CAM updates the entry as it receives new SNMP trap information for the client.

Removing an entry from the Wired Clients list clears this status information for the Out-of-Band client from the CAM.

Note An entry must exist in the Wired Clients list in order for the CAM to determine the switch port for which to change the VLAN. If the user is logging in at the same time that an entry in the Wired Clients list is deleted, the CAM will not be able to detect the switch port.

Figure 3-33 Discovered Clients


OOB Management > Devices
Devices
Discovered Clients
Wired Clients · Wireless Clients
(This page shows all the clients discovered from SNMP traps sent by Cisco Catalyst switches.)
Show clients connected to switch with IP: ALL
Show client with MAC:
Delete All Clients
Delete Selected
Clients/Page: 25
Clients 1-6 of 6 | First | Previous | Next | Last |
MAC | IP | Switch | Switch Port | Auth VLAN | Access VLAN | Last Update
00:14:22:9C:B0:C5 | N/A | 10.201.220.20 | 10010 | 50 | N/A | 2008-09-17 11:30:09.955
00:14:38:EB:B8:D3 | N/A | 10.201.220.51 | 10111 | 50 | N/A | 2008-09-17 12:40:05.361
00:14:6A:12:DA:66 | N/A | 10.201.220.20 | 10010 | N/A | N/A | 2008-09-17 11:30:10.085
00:14:6A:33:47:4E | N/A | 10.201.220.20 | 10002 | 50 | N/A | 2008-09-12 10:55:05.042
00:14:BF:5A:A7:A1 | 10.201.244.234 | 10.201.220.2 | 10038 | 55 | 220 | 2008-09-15 11:01:06.051
00:15:60:A3:6A:B1 | N/A | 10.201.220.51 | 10108 | 50 | N/A | 2008-09-17 13:22:48.747
189236

Elements of the page are as follows:

- **Show clients connected to switch with IP**—Leave the default of ALL switches displayed, or choose a specific switch from the dropdown menu. The dropdown menu displays all managed switches in the system.
- **Show client with MAC**—Type a specific MAC address and press Enter to display a particular client.
- **Clients/Page**—Leave the default of 25 entries displayed per page, or choose from the dropdown menu to displays 50, 100, 200, or ALL entries on the page.
- **Delete All Clients**—This button removes all clients on the list.
- **Delete Selected**—This button only removes the clients selected in the check column to the far right of the page.
- Note that you can click any of the following column headings to sort results by that column:
  - **MAC**—MAC address of discovered client
  - **IP**—IP address of the client
  - **Switch**—IP of the originating managed switch. Clicking the IP address brings up the **OOB Management > Devices > Switch [IP] > Config > Basic** page for the switch.
  - **Switch Port**—Switch port of the client. Clicking the port number brings up the **OOB Management > Devices > Switch [IP] > Ports** configuration page for the switch.
  - **Auth VLAN**—Authentication (quarantine) VLAN
    A value of "N/A" in this column indicates that either the port is unmanaged or the VLAN ID for this MAC address is unavailable from the switch.

- **Access VLAN**—Access VLAN of the client.
  A value of "N/A" in this column indicates the Access VLAN ID is unavailable for the client. For example, if the user is switched to the Auth VLAN but has never successfully logged into Cisco NAC Appliance (due to wrong user credentials), this machine will never have been to the Access VLAN.
- **Last Update**—The last time the CAM updated the information of the entry.

See Out-of-Band Users, page 3-68 for additional details on monitoring Out-of-Band users.

Manage Switch Ports

Once a switch is added, the **Ports** and **Config** tabs/pages only appear after a switch is added to the **OOB Management > Devices > Devices > List**.

The Ports page is the central point of management for the ports on a switch. You can apply Port profiles to individual or multiple ports, change VLAN settings, bounce ports, and apply all changes to the switch configuration.

Switch ports that are not connected to clients typically use the unmanaged port profile. Switch ports connected to clients use managed port profiles. After switch ports are configured and the settings are saved by clicking the **Update** button, the switch ports need to be initialized by clicking the **Setup** button when the switch supports MAC notification.

Cisco NAC Appliance provides OOB support for Cisco IP Phone deployments where the port is a trunk port and the native VLAN is the data VLAN. The CAM can manage switch trunk ports in addition to switch access ports.

Note Because Cisco NAC Appliance can control switch trunk ports for OOB (starting from release 3.6(1)+), make sure the uplink ports for managed switches are configured as "uncontrolled" ports after upgrade. This can be done in one of two ways:

- Before upgrading, change the **Default Port Profile** for the entire switch to "uncontrolled" under **OOB Management > Devices > Devices > List > Config[Switch_IP] > Default Port Profile | uncontrolled**
- After upgrading, change the **Profile** to "uncontrolled" for the applicable uplink ports of the switch under **OOB Management > Devices > Devices > List > Ports [Switch_IP] | Profile**

This prevents unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.

Ports Management Page

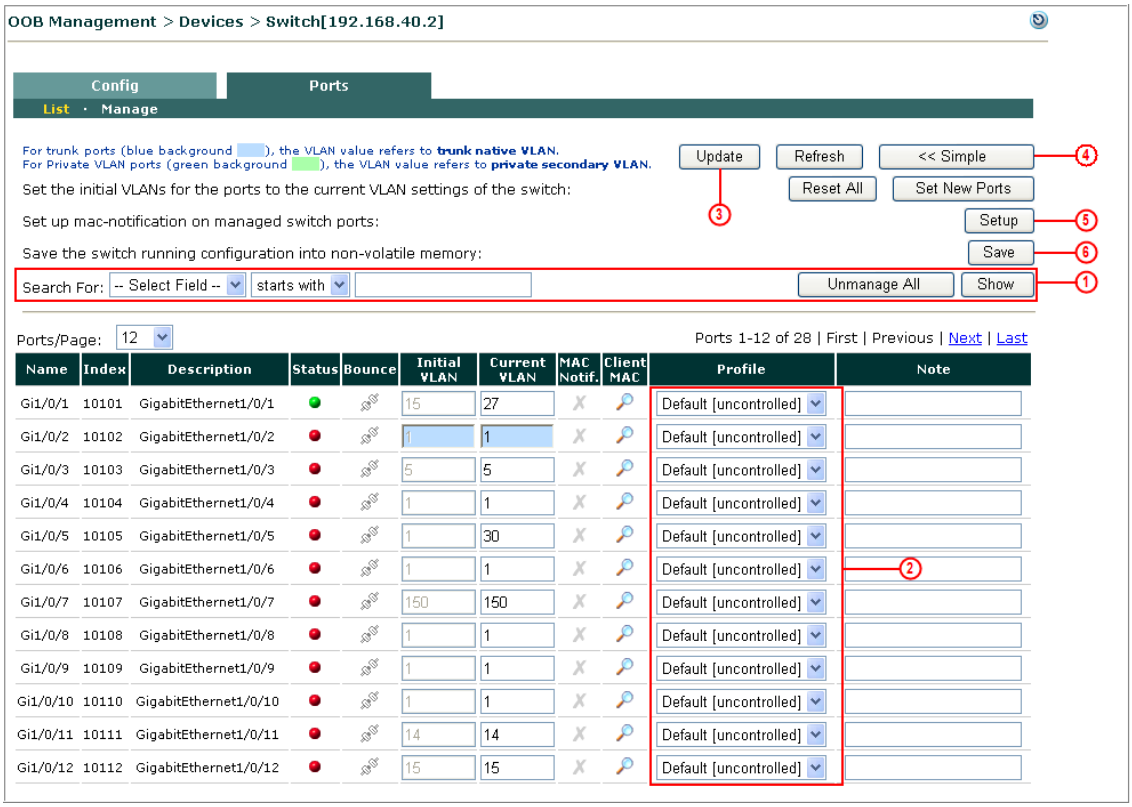
The **Ports** management page populates information for all Ethernet ports on a switch (see Figure 3-34 and Figure 3-35) according to the information the Clean Access Manager receives from direct SNMP queries. For example, if a switch added to the CAM has 24 Fast Ethernet ports and 2 Gigabit Ethernet uplinks, the **Ports** tab will display 26 rows, with one entry per port. Trunk ports configured on the switch are distinguished by blue background on the **Ports** page, and VLAN values for these ports refer to the trunk port native VLAN.

If the switch does not support MAC change notification/MAC move notification traps, the **Setup** button (**Set up mac-notification on managed switch ports**) and **MAC Notif.** column are not displayed on the page. In this case, linkup/linkdown traps must be supported and configured on the switch and Clean Access Manager. See Manage Individual Ports (Linkup/Linkdown), page 3-60 for the Ports management page controls for linkup/linkdown only ports.

Manage Individual Ports (MAC Notification)

This section describes the method you use to manage and/or assign a port profile to an individual switch port. This method works well for a small number of ports, but if you want to assign the same port profile to a large number of ports all at the same time, see Assign a Port Profile to Multiple Ports Simultaneously, page 3-62.

Figure 3-34 Ports Tab


OOB Management > Devices > Switch[192.168.40.2]
Config
Ports
List · Manage
For trunk ports (blue background), the VLAN value refers to trunk native VLAN.
For Private VLAN ports (green background), the VLAN value refers to private secondary VLAN.
Set the initial VLANs for the ports to the current VLAN settings of the switch:
Set up mac-notification on managed switch ports:
Save the switch running configuration into non-volatile memory:
Search For: -- Select Field -- starts with
Update
Refresh
<< Simple
Reset All
Set New Ports
Setup
Save
Unmanage All
Show
Ports/Page: 12
Ports 1-12 of 28 | First | Previous | Next | Last
Name Index Description Status Bounce Initial VLAN Current VLAN MAC Notif. Client MAC Profile Note
Gi1/0/1 10101 GigabitEthernet1/0/1 15 27 Default [uncontrolled]
Gi1/0/2 10102 GigabitEthernet1/0/2 1 1 Default [uncontrolled]
Gi1/0/3 10103 GigabitEthernet1/0/3 5 5 Default [uncontrolled]
Gi1/0/4 10104 GigabitEthernet1/0/4 1 1 Default [uncontrolled]
Gi1/0/5 10105 GigabitEthernet1/0/5 1 30 Default [uncontrolled]
Gi1/0/6 10106 GigabitEthernet1/0/6 1 1 Default [uncontrolled]
Gi1/0/7 10107 GigabitEthernet1/0/7 150 150 Default [uncontrolled]
Gi1/0/8 10108 GigabitEthernet1/0/8 1 1 Default [uncontrolled]
Gi1/0/9 10109 GigabitEthernet1/0/9 1 1 Default [uncontrolled]
Gi1/0/10 10110 GigabitEthernet1/0/10 1 1 Default [uncontrolled]
Gi1/0/11 10111 GigabitEthernet1/0/11 14 14 Default [uncontrolled]
Gi1/0/12 10112 GigabitEthernet1/0/12 15 15 Default [uncontrolled]
1
2
3
4
5
6
246963

After adding a new switch, set up the **Ports** configuration page (Figure 3-34) for the switch ports as follows:

Step 1 If you want to limit the switch profiles displayed in the Ports list, specify search criteria and click **Show** (•Show (1), page 3-57).

Step 2 Choose the **Profile** (•Profile (2), page 3-60) to use for the port, either managed or unmanaged.

Step 3 Click **Update** (•Update (3), page 3-57) to save the Port Profile for the port to the CAM.

Step 4 Click **Advanced/Simple** (4) toggle button to reveal the advanced port assignment features available for the switch ports.

Step 5 Click **Setup** (•Setup button (MAC notification switches only) (5), page 3-56) to initialize MAC change notification/MAC move notification on switch ports (if available on the switch).

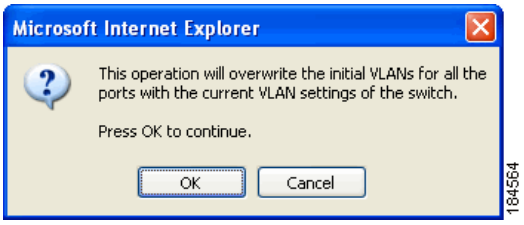
Step 6 Click **Save** (•Save (6), page 3-57) to save the switch running configuration to the switch stored (startup) configuration.

- **Unmanage All**

  Click **Unmanage All** to change all the managed ports to default port profile that was setup for the switch.

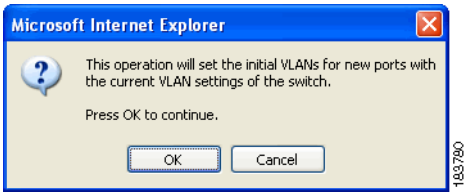
- **Reset All** (Initial VLAN Port Profiles only)

  Clicking **Reset All** copies the switch's **Current VLAN** values (•Current VLAN, page 3-59) for all ports and sets these as the **Initial VLAN** settings (for access ports) and trunk native VLAN settings (for trunk ports) (•Initial VLAN (Initial VLAN Port Profiles only), page 3-58) on the CAM and on the running configuration of the switch. This button allows you to change the Initial VLAN for all ports at the same time on the switch. Click **OK** in the confirmation to reset the values:


Microsoft Internet Explorer
This operation will overwrite the initial VLANs for all the ports with the current VLAN settings of the switch.
Press OK to continue.
OK
Cancel
184564

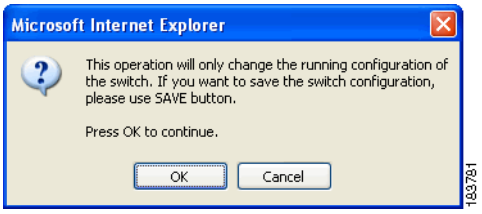
- **Set New Ports** (Initial VLAN Port Profiles only)

  Clicking **Set New Ports** (Figure 3-34) preserves settings for existing ports, but copies the switch's **Current VLAN** values for new ports and sets these as **Initial VLAN** settings (for access ports) and trunk native VLAN settings (for trunk ports) on the CAM and on the switch running configuration. This is useful when new ports are added to a switch, such as when adding a new blade in a Catalyst 4500 series rack. In this case, when the new ports are added, the **Initial VLAN** column displays "N/A." Clicking **Set New Ports** copies the values from Current VLAN column to the Initial VLAN column for all "N/A" ports and sets these values on the CAM and switch. The Initial VLAN values for existing ports on the switch (i.e. not "N/A") will not change. Click **OK** in the confirmation to set the new values.


Microsoft Internet Explorer
This operation will set the initial VLANs for new ports with the current VLAN settings of the switch.
Press OK to continue.
OK
Cancel
183780

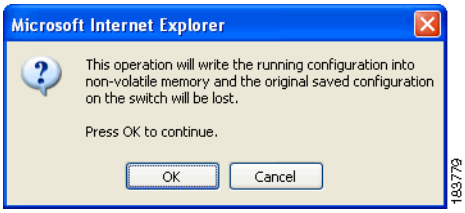
- **Setup** button (MAC notification switches only) **(5)**

  For switches that support MAC change notification/MAC move notification traps, click the **Setup** button after updating the CAM to set up MAC notification on managed switch ports and save the running configuration of the switch. Click **OK** to initialize ports on the switch.


Microsoft Internet Explorer
This operation will only change the running configuration of the switch. If you want to save the switch configuration, please use SAVE button.
Press OK to continue.
OK
Cancel
183781

- **Save (6)**

  Click the **Save** button to save the running configuration into non-volatile memory (startup configuration) on the switch. Click OK in the confirmation.


Microsoft Internet Explorer
This operation will write the running configuration into non-volatile memory and the original saved configuration on the switch will be lost.
Press OK to continue.
OK
Cancel
183779

Note The VLAN assignment of the port will not be changed in the startup configuration of the switch unless you click the **Save** button.

- **Update (3)**

  After you configure managed ports by choosing the applicable Port Profile, you must click the **Update** button to save these settings on the CAM. Clicking **Update** does the following:

  – Saves the Profile for the port to the CAM database.

  – Saves any Notes for the port to the CAM database.

  If the Port profile is configured with the **Initial Port VLAN** as the Access VLAN and set to "Change to **Access VLAN** if the device is certified and in the Out-of-Band user list," clicking **Update** also does the following:

  – Saves values in the Initial VLAN column for the port to the CAM database.

  – If the Current VLAN value of the port is changed, saves the new VLAN ID for the port to the running configuration of the switch.

- **Show (1)**

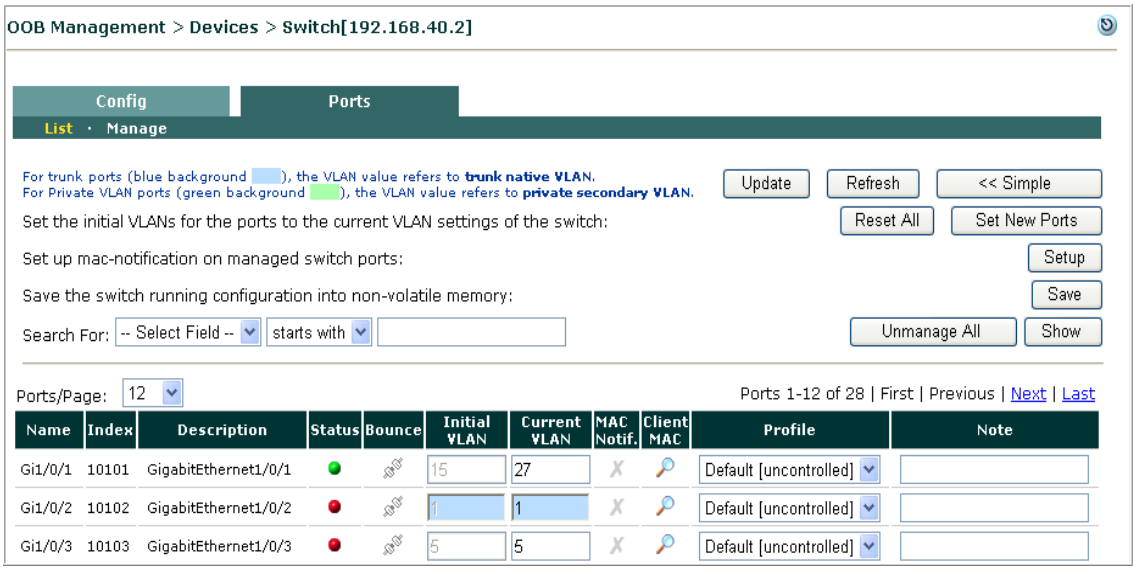
  To limit the range of switch ports displayed in the **Ports** tab view, you can specify search criteria using the **Search For** filtering functions and specify a text string for which to search. You can specify:

  – The information type to search—either the **Port Name** or **Port Description**

  – The information qualifier—select from **equals**, **starts with**, **ends with**, or **contains**

  – The test string defining the search (like "/11" in our example below)

  Once you have specified the search criteria, click **Show**.


OOB Management > Devices > Switch[192.168.40.2]
Config
Ports
List · Manage
For trunk ports (blue background), the VLAN value refers to trunk native VLAN.
For Private VLAN ports (green background), the VLAN value refers to private secondary VLAN.
Update
Refresh
<< Simple
Set the initial VLANs for the ports to the current VLAN settings of the switch:
Reset All
Set New Ports
Set up mac-notification on managed switch ports:
Setup
Save the switch running configuration into non-volatile memory:
Save
Search For: -- Select Field -- starts with
Unmanage All
Show
Ports/Page: 12
Ports 1-12 of 28 | First | Previous | Next | Last
Name Index Description Status Bounce Initial VLAN Current VLAN MAC Notif. Client MAC Profile Note
Gi1/0/1 10101 GigabitEthernet1/0/1 15 27 Default [uncontrolled]
Gi1/0/2 10102 GigabitEthernet1/0/2 1 1 Default [uncontrolled]
Gi1/0/3 10103 GigabitEthernet1/0/3 5 5 Default [uncontrolled]
246922

- **Name**

  Port name, for example: Fa0/1, Fa0/24, Gi0/1, Gi0/21 (for Cisco switches)

- **Index**

  The port number on the switch, for example: 1, 24, 25, 26

- **Description**

  Type of port, for example: FastEthernet0/1, FastEthernet0/24, GigabitEthernet0/1, GigabitEthernet0/2

- **Status**

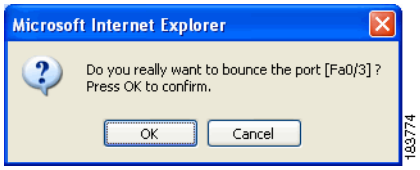
  Connection status of the port.

  – A green button indicates a device is connected to the port.

  – A red button means no device is connected to the port.

- **Bounce**

  Clicking this icon bounces an initialized, managed port. A confirmation appears before the port is bounced. Note that this feature is only available for managed ports. A port that is connected but not managed cannot be bounced. By default, this feature is disabled for trunk ports.



- **Initial VLAN** (Initial VLAN Port Profiles only)

  The Initial VLAN value saved by the CAM for this port. This column is only enabled for managed Port profiles configured with the **Initial Port VLAN** as the Access VLAN and set to "Change to Access VLAN if the device is certified and in the Out-of-Band user list" (see Add Port Profile,

page 3-34). When a switch is added, this column is identical to the Current VLAN column. When new ports are added to a switch, this column displays "N/A" for these ports until the **Set New Ports** button is clicked (•Set New Ports (Initial VLAN Port Profiles only), page 3-56).

To change the Initial VLAN of a port on-the-fly:

a. Make sure the port's Port profile is configured with the **Initial Port VLAN** as the Access VLAN and set to "Change to Access VLAN if the device is certified and in the Out-of-Band user list"

b. Type the modified VLAN for the port in the **Initial VLAN** field.

c. Click the **Update** button to save the changed configuration on the CAM.

See also: •Reset All (Initial VLAN Port Profiles only), page 3-56, •Set New Ports (Initial VLAN Port Profiles only), page 3-56, and •Save (6), page 3-57.

- **Current VLAN**

  The Current VLAN ID assigned to the port. When a new switch is added, the Current VLAN column reflects the VLAN assignments already configured on the switch by the network administrator. Thereafter, the values in this column are dynamic and reflect the current VLAN assignments on the switch (not necessarily the stored VLAN assignment). For trunk ports, the Current VLAN refers to the native VLAN of the trunk port.

  To change the Current VLAN assignment for a port on-the-fly:

  a. Type the modified value for the port in the **Current VLAN** field.

  b. Click the **Update** button to save the changed configuration to the CAM and to the running configuration of the switch.

  c. Click the **Save** button to save the switch running configuration to the startup configuration of the switch.

  See also •Reset All (Initial VLAN Port Profiles only), page 3-56, •Set New Ports (Initial VLAN Port Profiles only), page 3-56, and •Save (6), page 3-57.

- **MAC Notif.**

  MAC notification capability. The presence of this column indicates the switch is using SNMP MAC change notification/MAC move notification traps. If the switch does not support MAC notification traps, or if linkup notification is chosen in the Advanced configuration page (see Advanced, page 3-64), the **MAC Notif.** column and **Setup** button are not displayed on the **Ports** config page. In this case, linkup/linkdown traps must be used.

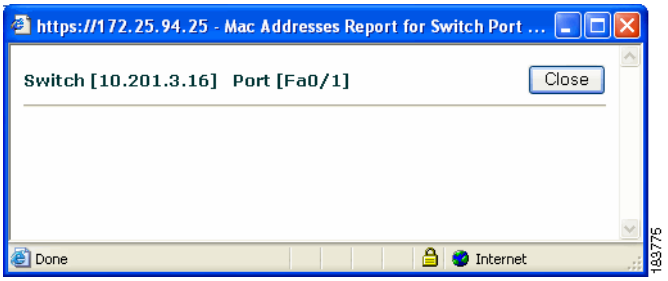
  – A green check in the **Mac Notif.** column means the corresponding port on the switch is enabled for this trap.

  – A grey x means the port has not been enabled for this trap, or is not managed.

  – A red exclamation point (!) next to either a green check or a grey x means an inconsistency exists between the port configuration on the switch and the port configuration in the Clean Access Manager. Exclamation points will appear after clicking **Update** and before clicking **Setup** to prompt the user to resolve the inconsistencies before attempting to save the settings to the switch.

- **Client MAC**

  Clicking this button brings up a dialog with the MAC address of the client attached to this port, the IP address of the switch, and the Name of the port to which the client is connected. For a managed port, only one MAC address displays for the attached client device. For unmanaged ports, this dialog displays all the MAC addresses associated with this port, but will not indicate where the MAC addresses are located (could be on other switches).



Note The MAC address(es) connected to a particular port may not be available when the Access VLAN of the port does not exist in the VLAN database. This occurs on some models of Cisco switches (e.g. 6506, IOS Version 12.2(18) SXD3).

- **Profile (2)**

  To control a port from the CAM, select a managed port profile from the dropdown menu, then click **Update** and **Setup**. Apply managed port profiles to ports on which clients are attached in order to get and set the SNMP traps from those ports. Profiles can also be applied to trunk ports. All other ports should be unmanaged. Port Profiles must already be configured under **OOB Management > Profiles > Port > New** (see Configure Port Profiles, page 3-33). There are always two default dropdown options: uncontrolled, and Default []. All ports are initially assigned the Default[uncontrolled] Port Profile. You can change the Default [] Port Profile assignment from the **OOB Management > Devices > Config** tab.

Note Because Cisco NAC Appliance OOB can control switch trunk ports, when upgrading, make sure uplink ports for managed switches are configured as "uncontrolled" ports. You can do this before upgrade by making sure the Default Port Profile for the entire switch is "uncontrolled" under **OOB Management > Devices > Devices > List > Config[Switch_IP] > Default Port Profile** (see Config Tab, page 3-63), or, after upgrade, you can change the **Profile** here in the **Ports** config page to "uncontrolled" for the applicable uplink ports of the switch.This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.

- **Note**

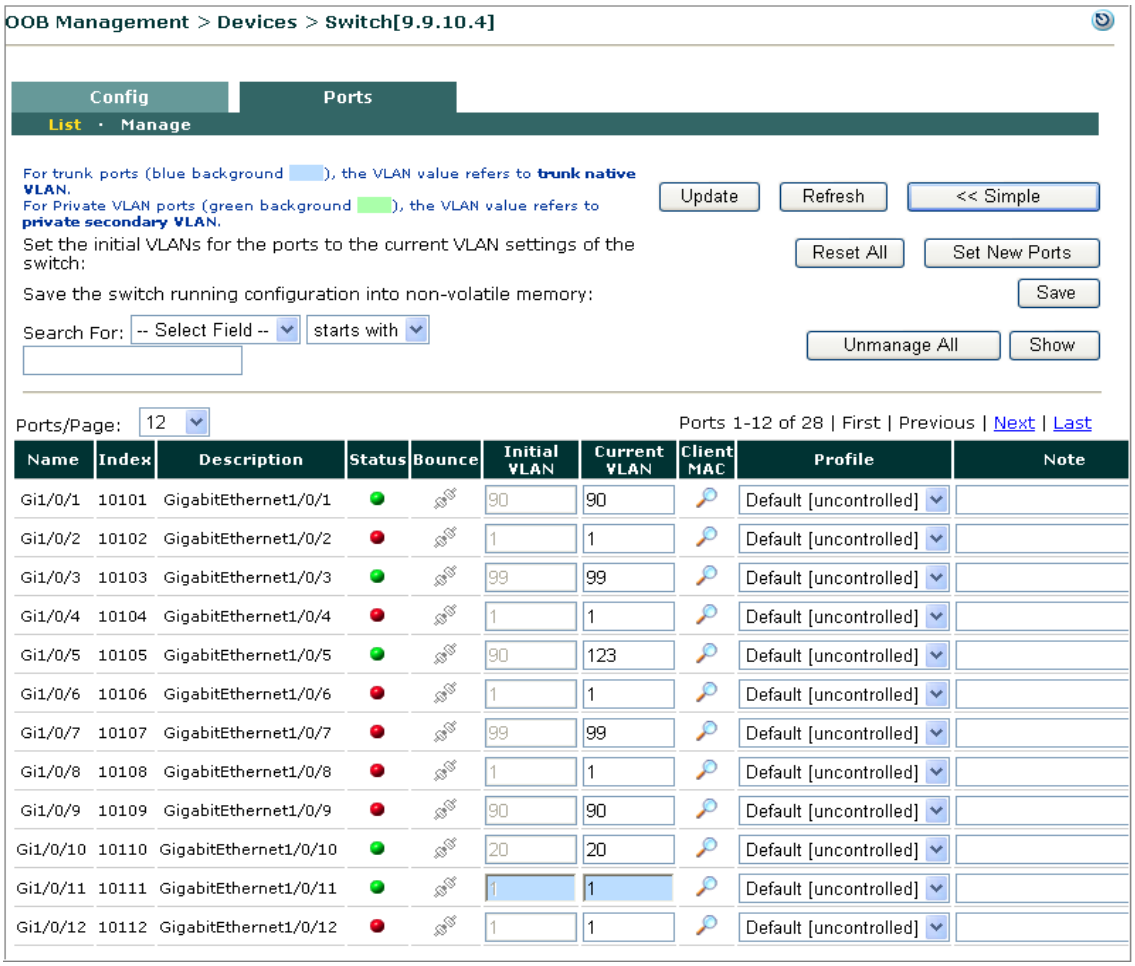
  This field allows you enter an optional description for ports you configure. Clicking **Update** saves the note for the port on the CAM.

Manage Individual Ports (Linkup/Linkdown)

If the switch does not support MAC change notification/MAC move notification traps, the **Mac Notif.** column and **Setup** button are not displayed on this page (Figure 3-35). In this case, linkup/linkdown traps must be supported and configured on the switch and Clean Access Manager.

See Advanced, page 3-64 for additional information on the use of linkup/linkdown traps.

Figure 3-35 Ports Tab—Linkup/Linkdown

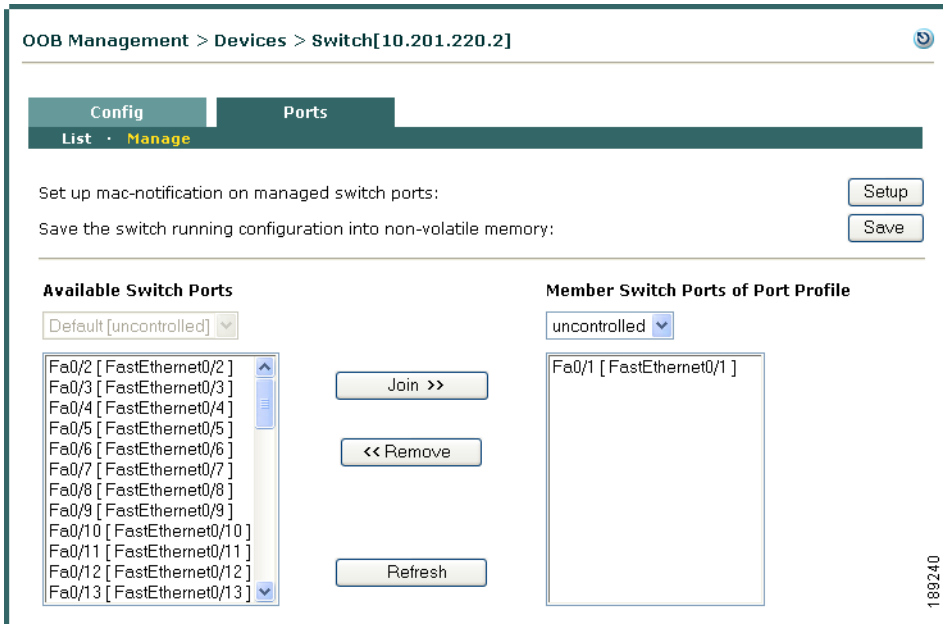

OOB Management > Devices > Switch[9.9.10.4]
Config
Ports
List · Manage
For trunk ports (blue background), the VLAN value refers to trunk native VLAN.
For Private VLAN ports (green background), the VLAN value refers to private secondary VLAN.
Update
Refresh
<< Simple
Set the initial VLANs for the ports to the current VLAN settings of the switch:
Reset All
Set New Ports
Save the switch running configuration into non-volatile memory:
Save
Search For: -- Select Field -- starts with
Unmanage All
Show
Ports/Page: 12
Ports 1-12 of 28 | First | Previous | Next | Last
Name Index Description Status Bounce Initial VLAN Current VLAN Client MAC Profile Note
Gi1/0/1 10101 GigabitEthernet1/0/1 90 90 Default [uncontrolled]
Gi1/0/2 10102 GigabitEthernet1/0/2 1 1 Default [uncontrolled]
Gi1/0/3 10103 GigabitEthernet1/0/3 99 99 Default [uncontrolled]
Gi1/0/4 10104 GigabitEthernet1/0/4 1 1 Default [uncontrolled]
Gi1/0/5 10105 GigabitEthernet1/0/5 90 123 Default [uncontrolled]
Gi1/0/6 10106 GigabitEthernet1/0/6 1 1 Default [uncontrolled]
Gi1/0/7 10107 GigabitEthernet1/0/7 99 99 Default [uncontrolled]
Gi1/0/8 10108 GigabitEthernet1/0/8 1 1 Default [uncontrolled]
Gi1/0/9 10109 GigabitEthernet1/0/9 90 90 Default [uncontrolled]
Gi1/0/10 10110 GigabitEthernet1/0/10 20 20 Default [uncontrolled]
Gi1/0/11 10111 GigabitEthernet1/0/11 1 1 Default [uncontrolled]
Gi1/0/12 10112 GigabitEthernet1/0/12 1 1 Default [uncontrolled]
246921

Assign a Port Profile to Multiple Ports Simultaneously

If your switch configuration includes many access ports that all feature the same port profile assignments to provide remote users authentication and access to the network, you can use the **OOB Management > Devices > Switch [x.x.x.x] > Ports > Manage** page to assign the same port profile to many switch ports all at the same time. If you have only a couple or few ports to which you must assign port profiles, see the procedure in Manage Individual Ports (MAC Notification), page 3-55.

Step 1 Go to **OOB Management > Devices > Switch [x.x.x.x] > Ports > Manage** (Figure 3-36).

Figure 3-36 OOB Management > Devices > Switch [x.x.x.x] > Ports > Manage



Step 2 Select the existing port profile you want to assign to the target switch ports from the **Member Switch Ports of Port Profile** dropdown menu.

Step 3 Highlight one or more switch ports in the **Available Switch Ports** list to which you want to assign the specified port profile.

Step 4 Click **Join >>**.

Step 5 Click **Setup** (•Setup button (MAC notification switches only) (5), page 3-56) to initialize MAC change notification/MAC move notification on switch ports (if available on the switch).

Step 6 Click **Save** (•Save (6), page 3-57) to save the switch running configuration to the switch stored (startup) configuration.

Config Tab

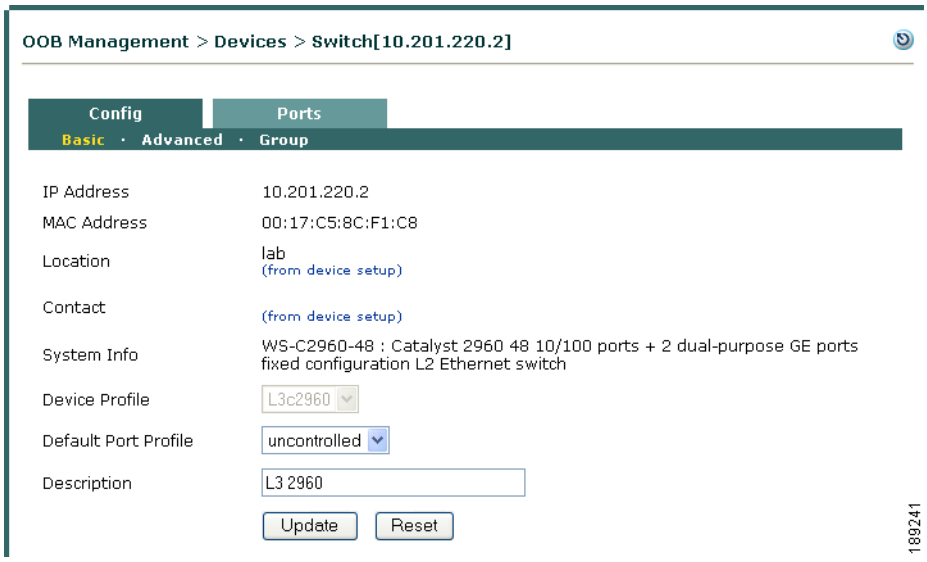
The Config tab allows you to modify Basic, Advanced, and Group profile settings for a particular switch:

- Basic
- Advanced
- Group

Basic

The Basic tab (Figure 3-37) shows the following values configured for the switch.

Figure 3-37 Basic Config



- The first values come from the initial configuration done on the switch itself:
  - IP Address
  - MAC Address
  - Location
  - Contact
  - System Info (translated from the MIB for the switch)
- **Device Profile**—Shows the Device Profile you are using for this switch configured under **OOB Management > Profiles > Device**. The Device Profile sets the model type, the SNMP port on which to send SNMP traps, SNMP version for read and write and corresponding community strings, or authentication parameters (SNMP V3 Read and Write).
- **Default Port Profile**—Shows the default Port profile applied to unconfigured ports on the switch on the **Ports** tab. The "uncontrolled" port profile is the initial default profile for all ports, unless you change the setting here. You can change the Default Port Profile by selecting another profile from the dropdown menu and clicking **Update**.

Note Because Cisco NAC Appliance OOB can control switch trunk ports, when upgrading, make sure uplink ports for managed switches are configured as "uncontrolled" ports. You can do this before upgrade by making sure the Default Port Profile for the entire switch is "uncontrolled" here, or, after upgrade you can change the Profile to "uncontrolled" for the applicable uplink ports of the switch under **OOB Management > Devices > Devices > List > Ports [Switch_IP] | Profile** (see Ports Management Page, page 3-54). This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile

- **Description**—Optional description of the switch. To change this field, type a new description and click **Update**.

Advanced

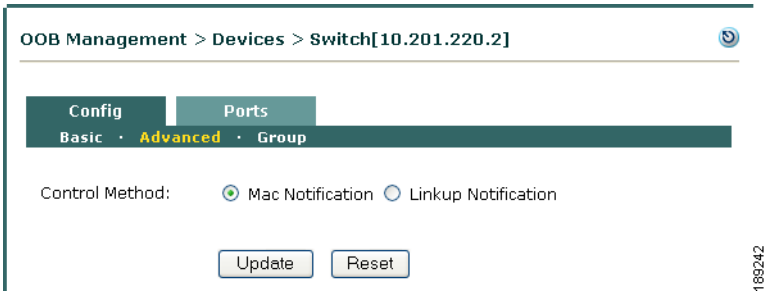
Use the Advanced Config page (Figure 3-38) to view or configure which SNMP trap notification type the CAM SNMP Receiver will use for a particular switch.

- **MAC Notification**—If a switch supports MAC Notification, the CAM automatically enables this option.

Note To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- **Linkup Notification**—If a switch does not support MAC Notification, the CAM enables the Linkup Notification option instead. In this case the administrator can optionally enable **Port Security** on the switch if the switch supports this feature. See Port Security, page 3-65 for additional details.
- If a switch supports both **MAC Notification** and **Linkup Notification**, the administrator can optionally disable MAC notification by selecting **Linkup Notification** instead and clicking **Update**.

Figure 3-38 Advanced Config



Linkup/linkdown is a global system setting on the switch that tracks whether a connection has non-operating or operating status. With the linkup/linkdown trap method, the Clean Access Manager must poll each port to determine the number of MAC addresses on the port.

Linkdown Traps

A client machine shutdown or reboot triggers a linkdown trap sent from the switch to the CAM (if linkdown traps are set up on the switch and configured on the CAM via the Port profile). Thereafter, the client port behavior depends on the Port profile settings for that specific port.

Whether the SNMP receiver is configured for MAC notification or linkup, the CAM uses the linkdown trap to remove users. For example, the linkdown trap is used if:

- An OOB online user is removed and the Port Profile is configured with the **Kick Out-of-Band online user when linkdown trap is received** option.
- Port Security is enabled on the switch.

Port Security

Port Security is a switch feature that restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.

When you change the SNMP control method from **Mac Notification** to **Linkup Notification**, as described in Enabling Port Security, the **Port Security** checkbox will appear on the **Advanced** page (Figure 3-39) if the switch supports the feature. When using linkup notification, the Port Security feature can provide additional security by causing the port to only allow one MAC address when a user authenticates. So even if the port is connected to a hub, only the first MAC that is authenticated is allowed to send traffic. Note that availability of the Port Security feature is dependent on the switch model and OS being used.

When you enable Port Security on the CAM, the switch configuration is not immediately changed. Instead, when the next client connects to that port, the switch will add the configuration for the port which turns on Port Security for that MAC address. The switch will add that MAC address as the only MAC address allowed to connect to that port if other connection attempts are made.

Enabling Port Security

Step 1 Go to **OOB Management > Devices > List** and click the **Config** icon for the switch you want to control.

Step 2 From the **Config** tab, click the **Advanced** link.

Step 3 Click the option for **Linkup Notification**. A checkbox for **Port Security** appears if the switch supports the feature.

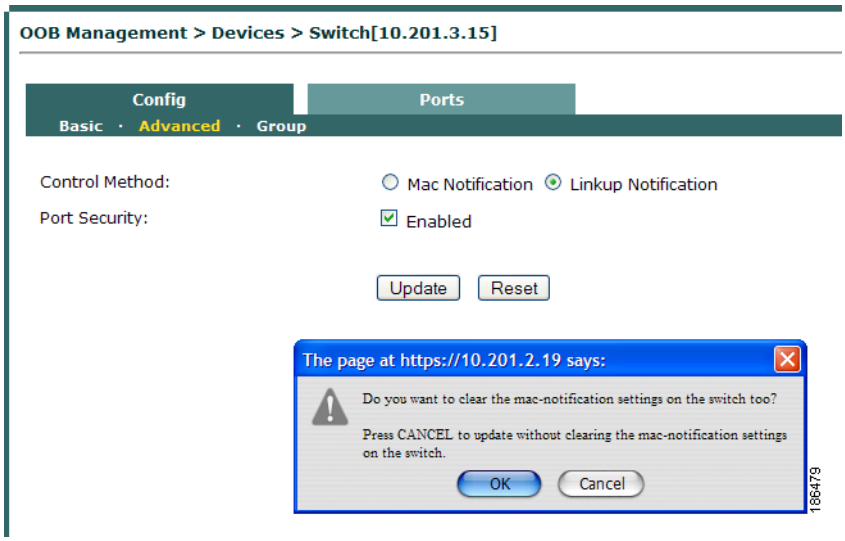
Step 4 Click the **Enable** checkbox for **Port Security**.

Step 5 Click **Update**.

Step 6 A prompt (Figure 3-39) appears with the following message: "Do you want to clear the mac-notification settings on the switch too? Press CANCEL to update without clearing the mac-notification settings on the switch."

- If you click **OK**, the CAM saves the Port Security setting and the "`snmp-server enable traps mac-notification`" line is removed from the switch configuration.
- If you click **Cancel**, the CAM saves the Port Security setting and the "`snmp-server enable traps mac-notification`" line is not removed from the switch configuration. This option can save some time if the administrator is planning to change the port back later to MAC Notification control. See Re-Enabling MAC Notification, page 3-66 for details.)

Figure 3-39 Enabling Port Security from the CAM



Note

- Port Security can only be enabled on a port set to Access mode (i.e not Trunk mode).
- The MAC address(es) connected to a particular port may not be available after Port Security is enabled. This occurs on some models of Cisco switches (e.g. 4507R, IOS Version 12.2(18) EW).
- If implementing High-Availability, ensure that Port Security is **not** enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

Re-Enabling MAC Notification

Step 1 Go to **OOB Management > Devices > List** and click the **Config** icon for the switch you want to control.

Step 2 From the **Config** tab, click the **Advanced** link.

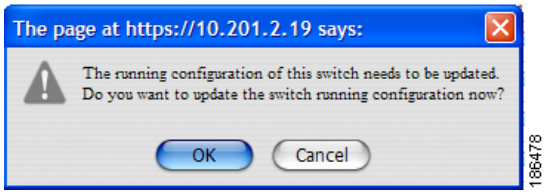
Step 3 Click the option for **Mac Notification**.

Step 4 Click **Update**.

Step 5 A prompt (Figure 3-40) displays the following message "The running configuration of this switch needs to be updated. Do you want to update the switch running configuration?"

- If you click **OK**, the running configuration is updated on the switch.
- If you click **Cancel**, you will need to reconfigure the controlled ports on the Ports page, as described Manage Individual Ports (MAC Notification), page 3-55.

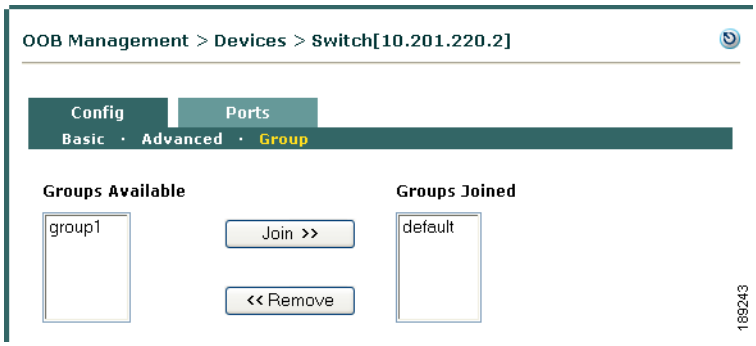
Figure 3-40 Reverting to MAC Notification from the CAM


The page at https://10.201.2.19 says:
The running configuration of this switch needs to be updated.
Do you want to update the switch running configuration now?
OK
Cancel
186478

Group

This page displays all the Group Profiles configured in the Clean Access Manager, and the Group Profiles to which the switch currently belongs. You can add the switch to other Groups, or you can remove the switch from a Group Joined. To change the Group membership for all switches, go to **OOB Management > Profiles > Group** (see Configure Group Profiles, page 3-28).

Figure 3-41 Config Group



Configure Access to Authentication VLAN Change Detection

Caution The Access to Authentication VLAN Change Detection feature should only be used for OOB deployments that require client DHCP IP refresh/renew. DHCP refresh/renew is configured under **Administration > User Pages > Login Page > List > Edit > General | Use web client to release and renew IP address when necessary (OOB)**. If your OOB deployment makes use of port bouncing, this feature is not needed and should not be configured. Refer to DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6 for additional details.

For In-Band clients and Out-of-Band clients which are still assigned to the Authentication VLAN, the Agent uses SWISS discovery packets to verify connectivity with the CAS. Once a client machine is on the Out-of-Band network and no longer communicates directly with the CAS, additional configuration is required for the client to determine whether it is still on the Access VLAN or moved to the Authentication VLAN. Versions prior to the 4.1.3.0 Agent cannot identify that the client port has switched from the Access VLAN to the Authentication VLAN and require the client machine's DHCP lease to run out in order to force the Agent to perform a DHCP release/renew to get a new IP address assignment.

To ensure OOB users are able to maintain network connection when the Cisco NAC Appliance administrator is forced to "kick" users out (and move the session back to the Authentication VLAN), you can configure the Cisco NAC Appliance system to have the Agent renew the IP address via DHCP release/renew.

This VLAN change detection behavior applies to the following scenarios:

- L3 OOB (Real-IP or Virtual Gateway)
- L2 OOB Real IP Gateway
- L2 OOB Virtual Gateway with user-role based VLAN assignment

If the Agent detects a change, the client machine automatically refreshes its IP address via DHCP release/renew. By default, the Agent automatically polls for the VLAN assignment on the switch every 5 seconds. If you want to increase or decrease that interval, users can adjust the "VlanDetectInterval" client setting.

For OOB deployments that require a client IP change, when the user is logged out and the client port changes from the Access VLAN to the Authentication VLAN, the IP address for the client machine also needs to change to come from the Authentication VLAN. In OOB, when the user is in the Access VLAN, the Agent no longer communicates with the CAM or CAS, so the Agent is not aware when the CAM changes the VLAN for the client port. Although the CAM can bounce the port to change the IP address on the client, this solution is not recommended for IP Phone environments, as it can disrupt voice services.

To enable and specify settings to support Access to Authentication VLAN Change Detection on a Windows client with the Cisco NAC Agent installed:

Step 1 Determine what settings you want to specify for the "RetryDetection," "PingArp," "PingMaxTimeout," or "VlanDetectInterval" parameters to enable the Access to Authentication VLAN Change Detection feature within your network and the **NACAgentCFG.xml** Agent configuration file accordingly. (See Cisco NAC Agent XML Configuration File Settings, page 9-23.)

Note VLAN Detect may fail when using ARP as discovery method in situations with high network utilization. Use ICMP as an alternative method.

Step 2 After you have specified the settings you want to use to guide Windows Cisco NAC Agent behavior, save the **NACAgentCFG.xml** Agent configuration file locally, upload it to the CAM, and make this new version available to Windows client machine users when they next authenticate with Cisco NAC Appliance (see Installation Page, page 9-20 for more information).

Note The Cisco NAC Agent only requires administrative privileges on the client machine during initial installation. Once successfully installed on the client machine, the Cisco NAC Agent does not require the user to have the administrative privileges to perform functions like Access to Authentication VLAN Change Detection.

Note For details on configuring the "VlanDetectInterval" setting on Windows and Mac OS X Cisco NAC Agent client machines, refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

Out-of-Band Users

OOB User Sessions

The following triggers detect when an OOB user has logged off and will force revalidation:

- Linkdown SNMP traps (when user unplugs or reboot)

- MAC notification traps

Note To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- Certified Timer expiration
- Session Timer expiration
- Manual removal from CAM

For additional details, see also Interpreting Event Logs, page 13-4 and Manage Certified Devices, page 11-10.

Wired and Wireless User List Summary

Table 3-4 describes the lists used to track wired and wireless users.

Table 3-4 Wired and Wireless User List Summary

User List	Description
In-Band Online Users	• The **In-Band Online Users** list (Figure 11-24 on page 11-31) tracks In-Band users logged into the network. • The CAM adds a client IP/MAC address (if available) to this list after a user logs into the network either through web login or the Agent. • Removing a user from this Online Users list logs the user off the In-Band network.
Certified Devices List	• The **Certified Devices List** (Figure 11-10 on page 11-13) lists the MAC addresses of all "certified" client devices—whether Out-of-Band or In-Band—that have met Agent requirements. • The CAM adds a client MAC address to the Certified Devices List after a client device goes through posture assessment and meets Agent requirements. • Removing a client from the Certified Devices List: – Removes an In-Band user from the **In-Band Online Users** list – Removes an OOB user from the **Out-of-Band Online Users** list (causing the port to be changed from the Access VLAN to the Authentication VLAN) and bounces the port, unless **Remove Out-of-Band online user without bouncing the port** is checked for the Port profile.

Table 3-4 Wired and Wireless User List Summary

User List	Description
Wired Clients and **Wireless Clients**	• The **Wired Clients** and **Wireless Clients** lists (Figure 3-33 on page 3-53 and Figure 4-20 on page 4-24) record the activities of Out-of-Band clients (regardless of VLAN), based on the SNMP trap information that the CAM receives. • For Wired OOB clients, the CAM adds a client's MAC address, originating switch IP address, and switch port number to the Out-of-Band Discovered Clients list after receiving SNMP trap information for the client from the switch. The CAM updates the entry as it receives SNMP trap information for the client. • For Wireless OOB clients, the CAM adds a client's MAC address, IP address, associated WLC, Access Point MAC address, and Authentication (Quarantine) and Access VLAN assignments to the Wireless Clients list. Thereafter, the CAM updates the entry as it receives new SNMP trap information for the wireless client. • Removing an entry from the Wired Clients or Wireless Clients list clears this status information for the OOB client from the CAM. **Note** For Wired OOB clients, an entry must exist in the Wired Clients list in order for the CAM to determine the switch port for which to change the VLAN. If the user is logging in at the same time that an entry in the Discovered Clients list is deleted, the CAM will not be able to detect the switch port.
Out-of-Band Online Users	• The **Out-of-Band Online Users** list (Figure 11-25 on page 11-32) tracks all authenticated Out-of-Band users that are on the Access VLAN (on the trusted network). • The CAM adds the client MAC address to the Out-of-Band Online Users list after a client is switched to the Access VLAN. **Note** The "User IP" of an OOB online user is the IP address of the user on the Authentication VLAN. By definition Cisco NAC Appliance does not track users once they are on the Access VLAN; therefore OOB users are tracked by the Authentication VLAN IP address they have while in the Cisco NAC Appliance network. • When a user is removed from the Out-of-Band Online Users list, the CAM instructs the switch or Wireless LAN Controller to change the VLAN of the port from the Access VLAN to the Authentication VLAN. **Note** For Wired OOB clients, if the Cisco NAC Appliance system somehow terminates the OOB client session (if the system administrator is forced to "kick" the user out, for example) and the switch changes the VLAN assignment for the client's access port from the Access VLAN back to the Authentication VLAN, the client machine discovers the VLAN change and, if configured, initiates an IP address refresh/renew to ensure the user stays connected to the network. For details on the polling method and configuration guidelines, see Configure Access to Authentication VLAN Change Detection, page 3-67. • Additionally, if **Bounce the port after VLAN is changed** is checked for the Port Profile (Real-IP gateways), the following occurs: 1. The CAM bounces the switch port (off and on). 2. The switch resends SNMP traps to the CAM. 3. The CAM discovers the device connected to the switch port from SNMP MAC change notification/MAC move notification or linkup traps received. 4. The port is assigned the Auth VLAN if the device is not certified. 5. The CAM changes the VLAN of the port according to the Port Profile configuration

OOB Troubleshooting

- OOB Switch Trunk Ports After Upgrade, page 3-71
- OOB Error: connected device <client_MAC> not found, page 3-71
- OOB Error: connected device <client_MAC> not found, page 3-71

OOB Switch Trunk Ports After Upgrade

Because Cisco NAC Appliance can control switch trunk ports for OOB (starting from release 3.6(1) and above), uplink ports for managed switches need configured as "uncontrolled" ports either before or after upgrade (see "Settings That May Change With Upgrade" in the corresponding *Release Notes for Cisco NAC Appliance*.

This can be done in one of two ways:

- Before upgrading, change the **Default Port Profile** for the entire switch to "uncontrolled" under **OOB Management > Devices > Devices > List > Config [Switch_IP] > Default Port Profile | uncontrolled**
- After upgrading, change the **Profile** to "uncontrolled" for the applicable uplink ports of the switch under **OOB Management > Devices > Devices > List > Ports [Switch_IP] | Profile**

This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile

If for some reason the above steps are omitted and the switch becomes disconnected, use the following procedure:

Step 1 Delete the switch from the List of Switches in the CAM (under **OOB Management > Devices > Devices > List**).

Step 2 Configure the switch using its CLI to reverse the changes made to the uplink port by the CAM (trunk native VLAN and MAC change notification/MAC move notification), for example:

```
(config-if)# switchport trunk native vlan xxx
(config-if)# no snmp trap mac-notification added
```

Step 3 Add the switch back to the CAM (under **OOB Management > Devices > Devices > New** or **Search**), applying "uncontrolled" as the Default Port Profile.

Step 4 Specifically assign the "uncontrolled" port Profile to the uplink port and other uncontrolled ports (under **OOB Management > Devices > Devices [x.x.x.x] > Ports**).

Step 5 Reset the Default Port Profile for the switch (under **OOB Management > Devices > Switches [x.x.x.x] > Config**).

Initialize the switch ports (under **OOB Management > Devices > Devices [x.x.x.x] > Ports**).

OOB Error: connected device <client_MAC> not found

Client connection errors can result from incorrect configuration of the switch profile. If attempting to log into the network using the Agent, and the Agent provides the following error: "**Login Failed! OOB Error: connected device <client_MAC> not found. Please contact your network administration.**"

- Make sure the switch profile matches the switch type under **OOB Management > Devices > Devices > New**

  For example, if the switch is a 3750, but you specified it a 2950 switch profile when adding the switch, when the CAM receives the SNMP linkup trap from the switch for the client that is connecting (with the MAC address specified in the Agent error message), the CAM will attempt to contact that switch to find that MAC address. If the wrong profile is specified for the switch, or the switch is not yet configured in the CAM, the CAM will not be able to contact that switch. Changing the switch profile to 3750 will resolve this issue.

Troubleshooting SNMP

This section describes how to troubleshoot the common errors that occur in SNMP operations.

Device IP Not Reachable, page 3-72
Fetching SysObjectID, page 3-72
SNMP Request Timed Out, page 3-72
Unknown User Name, page 3-73
Wrong Digest, page 3-73
Authorization Error, page 3-73
Unsupported Security Level, page 3-73
No Access, page 3-73
OOB Client MAC/IP Not Found, page 3-74
Message Not Within Time Window, page 3-74
Additional Information, page 3-74

Device IP Not Reachable

Error: The device IP is not reachable. Please check the device IP and try again.

This error may occur while adding a switch to CAM. This happens when the switch IP is not reachable from CAM. Check the network connectivity between the CAM and the switch.

Fetching SysObjectID

Error fetching the sysobjectid of the device <switch-ip-address>. Please check the SNMP settings on the device. They should match the SNMP settings defined in the device profile.

This happens when the SNMP read settings on the device do not match with the settings configured in the CAM under **OOB Management > Profiles > Device**.

SNMP Request Timed Out

Error: SNMP request timed out [1.3.6.1.4.1.9.9.215.1.1.5.0]

CAM logs contain the error as shown in the following example:

```
2012-01-08 18:41:57.010 +0530 [TP-Processor23] ERROR com.perfigo.wlan.web.sms.Switch
- switch [9.0.20.3] SNMP WRITE failed, 1 consecutive write failures!
2012-01-08 18:41:57.011 +0530 [TP-Processor23] ERROR com.perfigo.wlan.web.sms.SnmpManager
```

This error happens when there is a mismatch in the SNMP Write settings. When the admin clicks the ports for a switch, then this error is displayed in the CAM web console.

The SNMP Write settings setup in the device profile under **OOB Management > Profiles > Device** are different from the settings in the switch configuration. Make sure the settings are the same.

Unknown User Name

Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Unknown user name

This error occurs when the SNMP V3 username mentioned in the device profile under **OOB Management > Profiles > Device** does not exist in the switch configuration.

Wrong Digest

Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Wrong digest

This error occurs when the SNMP V3 Auth password or Auth type mentioned in the device profile under **OOB Management > Profiles > Device** does not match with the one in the switch configuration.

Authorization Error

Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Authorization error

This error occurs when the SNMP V3 Auth/Priv is not setup in the device profile under **OOB Management > Profiles > Device**, while the username in the switch configuration has been setup with the Auth/Priv security level.

Unsupported Security Level

Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: Unsupported Security Level

This error occurs when the SNMP V3 Auth/Priv is setup in the device profile under **OOB Management > Profiles > Device**, while the username in the switch configuration is not using any Auth/Priv security level.

No Access

Error: SNMP failure [1.3.6.1.4.1.9.9.215.1.1.5.0]: No access

This occurs when SNMP V3 user is not properly configured.

While creating a SNMP V3 user on the switch, the commands must be executed in the right order. The following order is recommended:

1. Create SNMP View
2. Create SNMP Group

3. Create SNMP User

If there is a change in the above order, then the user is not properly bound to the correct Group or View. This causes issues to the user and throws the above error.

OOB Client MAC/IP Not Found

Invalid Switch Configuration-OOB Error: OOB Client MAC/IP not found. Please contact network administrator.

This error usually occurs when the user tries to login. This happens when CAM is not able to find a matching entry for the client's MAC address in the Discovered Clients list

Perform the following steps:

- Check whether the SNMP receiver settings that are defined in CAM under **OOB Management > SNMP Receiver > SNMP Trap** match those defined in the switch configuration. Make sure that the switch is configured to send traps to CAM.
- Perform port bounce on the port to which the user is connected. This would make the switch to send the traps to CAM. On processing the traps, CAM would add an entry to the Discovered Clients list.

After performing the above, the user will be able to login successfully.

Message Not Within Time Window

Error: Message not within time window

This error is seen in packet captures performed at CAM when SNMP V3 is used for write operations. CAM stores the **`snmpEngineID`**, **`snmpEngineBoots`** and **`snmpEngineTime`** for every switch in its memory. When a switch is re-configured then the **`engineBoots`** and **`engineTime`** are reset. When the switch sends request, then these values are matched with the values that are stored in CAM for that **`engineID`**. If they are different, then the error message "Message not within time window" is displayed.

Workaround:

Update the switch profile. Go to the device profile under **OOB Management > Profiles > Device** for the corresponding switch and update it. This would allow the CAM to reset the **`engineBoots`** and **`engineTime`** for the switches to default values. Another workaround is to restart the CAM perfigo service.

Note Ensure that the switches are not configured with the same **`engineID`**. This causes the CAM to send the **`engineBoots`** and **`engineTime`** of one switch to another switch as the **`engineIDs`** are same. This results in failure of SNMP write operations and the error "message not in time window".

Additional Information

In the CAM web console, navigate to **OOB Management > Profiles > Port > New**. When the option **Generate event logs when there are multiple MAC addresses detected on the same switch port** is enabled, there may be an impact on performance, as hub detection happens for every SNMP trap. Make sure this option is disabled when using switches with large number of ports like 6500.



Wireless LAN Controller Management: Configuring Wireless Out-of-Band Deployment

This chapter describes how to configure Cisco NAC Appliance for Wireless Out-of-Band (Wireless OOB) deployment. Topics include:

- Overview, page 4-1
- Wireless Out-of-Band Virtual Gateway Deployment, page 4-5
- Configure Your Network for Wireless Out-of-Band, page 4-7
- Configure Your Wireless LAN Controllers, page 4-7
- Configure Wireless LAN Controller Connection on the CAM, page 4-13
- Wireless Out-of-Band Users, page 4-27

See *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for additional information on OOB deployments.

Overview

In a traditional In-Band Cisco NAC Appliance wireless deployment, all network traffic to or from wireless client machines passes through the Clean Access Server (CAS). For high throughput or highly routed environments, a Cisco NAC Appliance Wireless Out-of-Band (Wireless OOB) deployment allows client traffic to pass through the network only in order to be authenticated and certified before being connected directly to the access network.

Wireless Out-of-Band can be configured in the following deployments:

- Layer 2 Virtual Gateway
- Layer 2 Real IP
- Layer 3 Real IP

Note Cisco NAC Appliance Release 4.8(1) and earlier versions support only Layer 2 Virtual Gateway deployment. All the above deployments are supported by Cisco NAC Appliance Release 4.8(2) and later.

Starting from NAC Appliance Release 4.9, the wireless OOB is supported for roaming as well. When the client machine roams, the connectivity is not lost.

Wireless Out-of-Band is supported in the following scenarios of roaming:

- **Bewteen Access Points:** When client roams from one Access Point to another within the same Wireless controller (WLC).
- **Intra-subnet:** When client roams from one WLC to another WLC, where Quarantine and Access VLANs are the same and have the same IP subnets. WLC-2 sends SNMP Trap to CAM notifying about the user mobility and CAM updates the database accordingly.
- **Inter-subnet:** When client roams from one WLC to another within different subnets.

This section discusses the following topics:

- Wireless In-Band Versus Out-of-Band, page 4-2
- Wireless Out-of-Band Requirements, page 4-2
- SNMP Control, page 4-4
- Summary Steps to Configure Wireless Out-of-Band, page 4-5

Wireless In-Band Versus Out-of-Band

Table 4-1 summarizes different characteristics of each type of deployment.

Table 4-1 Wireless In-Band vs. Out-of-Band Deployment

Wireless In-Band Deployment Characteristics	Wireless Out-of-Band Deployment Characteristics
The Clean Access Server (CAS) is always inline with user traffic (both before and following authentication, posture assessment and remediation). Enforcement is achieved through being inline with traffic.	The Clean Access Server (CAS) is inline with user traffic only during the process of authentication, assessment and remediation. Following that, user traffic does not come to the CAS. Enforcement is achieved through the use of SNMP to coordinate with Wireless LAN Controllers (WLCs) and to assign/reassign VLAN assignments.
The CAS can be used to securely control authenticated and unauthenticated user traffic.	The CAS can control user traffic during the authentication, assessment and remediation phase, but cannot do so post-remediation since the traffic is Out-of-Band.
Bandwidth restricted to maximum allowable throughput for installed Clean Access Server(s).	Out-of-Band bandwidth not restricted by Clean Access Servers in network, as all client traffic bypasses CASs once clients are authenticated.

Wireless Out-of-Band Requirements

Wireless Out-of-band implementation of Cisco NAC Appliance requires the following to be in place:

- Cisco Wireless LAN Controllers must be supported models that use at least the minimum supported version of IOS (supporting SNMP traps). See Table 4-2.
- Cisco Wireless LAN Controllers must be Layer 2 adjacent to the Clean Access Server(s) with which they interoperate to support wireless client login for Cisco NAC Appliance Release 4.8(1) and earlier versions.

- Clean Access Servers supporting wireless client login and authentication must be installed and configured in Virtual Gateway mode for Cisco NAC Appliance Release 4.8(1) and earlier versions.
- For Cisco NAC Appliance Release 4.8(2) and later, Cisco Wireless LAN Controllers must be configured in bridging mode to interoperate with Layer 3 Out-of-Band wireless client login. Refer to DHCP Bridging Mode, page 4-3.

Note Administrators can update the object IDs (OIDs) of supported WLCs through CAM updates (under **Device Management > Clean Access > Updates > Summary | Settings**). For example, if a new WLC of a supported model (Cisco 4400 Series) is released, administrators only need to perform Cisco Updates on the CAM to obtain support for the WLC OIDs, instead of performing a software upgrade of the CAM/CAS.

The update WLC OID feature only applies to existing models. If a new WLC series is introduced, administrators will still need to upgrade to ensure Wireless OOB support for the new WLCs. See Configure and Download Updates, page 9-14.

Note The supported mode of HREAP in Cisco NAC Wireless Out-Of-Band is central authentication, central switching. In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.
Local Switching is not supported with Cisco NAC Wireless OOB.

Note For the most current details on WLC model/IOS version support, refer to *Switch Support for Cisco NAC Appliance*.

Table 4-2 Supported Wireless LAN Controller Models

Supported Wireless LAN Controllers	Wireless LAN Controller Release	Cisco NAC Appliance Release
Cisco 4400 Series Wireless LAN Controllers	5.1 and later	4.9
Cisco 2000 Series Wireless LAN Controllers		
Cisco Catalyst 3750G Integrated Wireless LAN Controller		
Cisco Catalyst 6500/7600 Series Wireless Services Module (WiSM)		
Cisco Wireless LAN Controller Module		

DHCP Bridging Mode

To enable the DHCP bridging functionality on the controller, you must disable the DHCP proxy feature on the controller. By default, DHCP proxy is enabled.

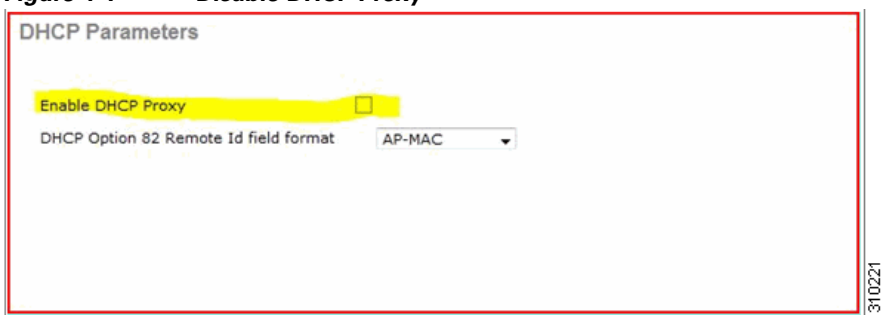
In the 4.2.x.x codes this can be done using the CLI using the following commands:

```
(Cisco Controller) > config dhcp proxy disable
(Cisco Controller) > show dhcp proxy
DHCP Proxy Behavior: disabled
```

The DHCP bridging feature is a global setting, so it affects all DHCP transactions within the controller. You need to add ip helper statements in the wired infrastructure for all necessary VLANs on the controller.

You can disable the DHCP proxy through the User Interface as well. In the WLC graphical user interface, click **Controller > Advanced > DHCP** and uncheck the **Enable DHCP Proxy** check box as shown in Figure 4-1.

Figure 4-1 Disable DHCP Proxy



Note Setting the DHCP Proxy using GUI is not available in all the versions. You can use the CLI command to disable the DHCP Proxy.

SNMP Control

In a Wireless OOB deployment, you can add WLCs to the Clean Access Manager's domain and communicate with the WLC using the Simple Network Management Protocol (SNMP). SNMP is an application layer protocol used by network management tools to exchange management information between network devices. Cisco NAC Appliance and Cisco WLCs support the following SNMP versions in a Wireless OOB environment:

CAM-to-OOB WLC SNMP Read	CAM-to-OOB WLC SNMP Write	OOB WLC-to-CAM SNMP Traps
• SNMP V1 • SNMP V2c (V2 with community string) • SNMP V3	• SNMP V1 • SNMP V2c • SNMP V3	• SNMP V2c

You first need to configure the WLC to send and receive SNMP traffic to/from the Clean Access Manager, then configure matching settings on the Clean Access Manager to send and receive traffic to/from the WLC. This will enable the Clean Access Manager to get VLAN information from the WLC and coordinate with the WLC when wireless users log out (or are "kicked out") of the network and removed from the Online Users list.

Summary Steps to Configure Wireless Out-of-Band

To enable Wireless OOB in you access network, you need to perform the following tasks:

1. Configure your Wireless LAN Controller:
   a. Enable SNMP read and write settings on the WLC.
   b. Enable SNMP trap transmission on the WLC using SNMP v2c (the SNMP v2c protocol is the only version of SNMP traps the CAM and WLCs have in common).
   c. Configure SSIDs/dynamic interfaces on the WLC with both an Authentication (Quarantine) VLAN and a standard Access VLAN.
2. Ensure SNMP settings on the CAM match those assigned on the WLC using the guidelines in Configure SNMP Receiver, page 4-19.
3. Create a new device profile on the CAM for the WLC using the guidelines in Add New Wireless LAN Controller, page 4-20.



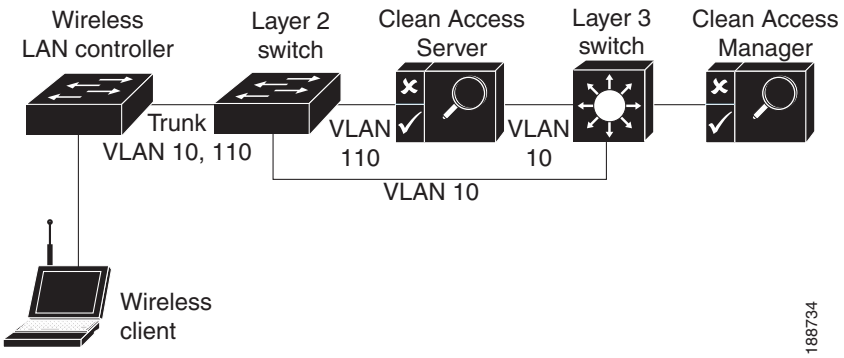
Note Unlike switch device profiles on the CAM, administrators do not configure or assign any Port Profiles for WLCs. VLAN assignments for Authentication (Quarantine) and Access VLANs originate form the WLC based on SNMP trap messages sent from the CAM following client posture assessment and remediation.

4. Add the new WLC device profile to the Device List using the guidelines in Add and Manage Wireless LAN Controllers, page 4-20.
5. Configure the CAS in your Cisco NAC Appliance network to support Wireless OOB network functions using the appropriate sections of the “Configuring the CAS Managed Network” chapter in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*:
   – Install the CAS according to the guidelines in the “Add New Server” section.
   – Ensure that the Cisco NAC Appliance system appropriately handles client traffic from the WLC’s Authentication (Quarantine) VLAN by using the “Configuring Managed Subnets or Static Routes” section.
   – Since the CAS acts as a bridge in Virtual Gateway mode, be sure the CAS is configured to map the WLC’s Access VLAN to the Cisco NAC Appliance Access VLAN (both on the Trusted VLAN) using the “Configure VLAN Mapping” section.

Wireless Out-of-Band Virtual Gateway Deployment

Figure 4-2 illustrates a typical Wireless OOB Virtual Gateway deployment. The WLC assigns two VLANs, AUthentication (Quarantine) VLAN 110 and Access VLAN 10, to one or more SSIDs/dynamic interfaces to support wireless client access. The WLC and the Layer 2 access switch have a VLAN trunk assignment for both VLANs so that client traffic automatically reaches the Layer 2 switch regardless of whether the wireless client machine has authenticated with Cisco NAC Appliance or not. The Layer 2 switch ensures that all unauthenticated traffic gets directed to the Clean Access Server via VLAN 110 and that authenticated clients remain Out-of-Band, thus bypasses the CAS and proceeding directly to the internal network via Access VLAN 10.

Figure 4-2 Wireless Out-of-Band Layer 2 VGW Mode



Login and Authentication Flow in Wireless OOB Virtual Gateway Mode

1. The unauthenticated wireless user connects to a Wireless LAN Controller through an associated wireless access point.
2. The WLC sends an association trap informing the CAM that a wireless user is logging in with Cisco NAC Appliance network access credentials.

   Note For Layer 3 Wireless OOB network, the MAC address of the device is added to the discovered clients list, when the WLC sends an association trap. When the user is logging in with the browser, the MAC address is detected. The MAC address detection is done using Java applet or ActiveX control.

   If the device cannot run Java applet or ActiveX, then the MAC address is not detected and this leads to error.

3. When the wireless client first logs into the Wireless OOB network, the user profile is assigned to Authentication (Quarantine) VLAN 110.
4. The CAS assigns the client machine an IP address from the access VLAN 10 and the WLC authenticates the client.

   Note If Single-Sign On (SSO) is configured for the Wireless OOB network, the WLC also sends the appropriate RADIUS accounting packets to the CAS.

   Cisco WLCs do not support IPSec communication with the Cisco NAC Appliance network, so you cannot provide RADIUS SSO capability to users in your FIPS 140-2 compliant environment.

5. Cisco NAC Appliance performs posture assessment and remediation on the client machine and, if the client machine meets security requirements, authenticates the client and sends an SNMP SET command to the WLC granting access to the internal network.
6. The WLC switches the client IP address from the Authentication (Quarantine) VLAN 110 to the Access VLAN 10 and (now that the client machine has authenticated with Cisco NAC Appliance) traffic between the wireless client machine and the internal network moves Out-of-Band, bypassing the CAS.

When the user logs out of the wireless OOB network, the WLC sends another SNMP update to the CAM to ensure the CAM removes the user profile from the wireless Online Users list. Likewise, if the Cisco NAC Appliance administrator is forced to "kick" a user out of the network, the CAM sends an SNMP trap to the WLC and the WLC, in return, automatically moves the user back to the Authentication (Quarantine) VLAN, thus directing the now unauthenticated client traffic to the CAS.

Configure Your Network for Wireless Out-of-Band

The CAM communicates with associated WLCs using SNMP and manages Wireless OOB CASs through the admin network. The trusted interface of the CAS connects to the admin/management network, and the untrusted interface of the CAS connects to the managed client network.

When a wireless client connects to a WLC, the WLC automatically assigns the client to an Authentication (Quarantine) VLAN and the traffic to/from the client goes through the CAS. After the client is authenticated and certified through the Clean Access Server, the WLC receives an SNMP message from the CAM allowing the client access to the network via the Access VLAN. Once on the access VLAN, traffic to and from certified clients moves Out-of-Band, bypassing the Clean Access Server.

The next sections describe the configuration steps needed to set up your Wireless OOB deployment:

- Configure Your Wireless LAN Controllers, page 4-7
- Configure Wireless LAN Controller Connection on the CAM, page 4-13

Configure Your Wireless LAN Controllers

This section describes the steps needed to set up Wireless LAN Controllers (WLCs) to be used with Cisco NAC Appliance for Wireless Out-of-Band.

- Wireless LAN Controllers Configuration Notes, page 4-7
- Example Wireless LAN Controller Configuration Steps, page 4-8
- Wireless OOB Network Setup/Configuration Worksheet, page 4-12

Wireless LAN Controllers Configuration Notes

The following considerations should be taken into account when configuring Wireless LAN Controllers for OOB:

- Cisco NAC Appliance only supports Wireless OOB deployments with Cisco Wireless LAN Controllers.
- WLCs must be configured to interact with the CAM using SNMP read, write, and trap functions.
- Each service set identifier (SSID)/dynamic interface on the WLC must have both an Authentication (Quarantine) VLAN and Access VLAN configured.
- When SSID is setup to perform Wireless SSO and there is a overlapping of IP subnets over multiple SSIDs, even after roaming from one SSID to another, the user is still listed under Online Users in the CAM. To avoid this, create separate IP ranges for each SSID.
- Ensure that any access/aggregation switches in the network between the WLCs and the Clean Access Server have the same Authentication (Quarantine) and Access VLANs trunked.

- Authentication and Access VLANs are defined on the WLC and changes between the two are transmitted to the CAM using SNMP traps—administrators do not assign VLANs from the CAM via user role assignments or otherwise.
- When a wireless user logs off, the WLC also sends SNMP information to the CAM to ensure the user ID is removed from the Online Users list. Likewise, if the administrator must kick any users out of the Online Users list, the CAM informs the WLC via SNMP and the WLC automatically assigns the wireless client to the Authentication (Quarantine) VLAN.
- If Single Sign-On (SSO) is required for wireless users, the WLC must also be configured to transmit RADIUS accounting packets to the CAS. Cisco WLCs do not support IPSec communication with the Cisco NAC Appliance network, so you cannot provide RADIUS SSO capability to users in your FIPS 140-2 compliant environment.

Note The VPN Auto Logout feature does not work in a Wireless OOB deployment. If VPN Auto Logout signs a user out of the system, the CAM will not learn of the disconnection from the WLC.

- If your wireless access network provides services for Wireless IP Phones, ensure you configure a separate SSID for such devices so that they do not encounter the Cisco NAC Appliance authentication process.

Example Wireless LAN Controller Configuration Steps

This section provides a configuration example for a Cisco 4400 series Wireless LAN Controller.

- Create the Dynamic Interface on the Wireless LAN Controller, page 4-8
- Create the WLAN on the Wireless LAN Controller and Enable Cisco NAC Appliance Integration, page 4-9
- Configure SNMP on the Wireless LAN Controller, page 4-10
- Specify the CAM as the SNMP Trap Receiver, page 4-11

Create the Dynamic Interface on the Wireless LAN Controller

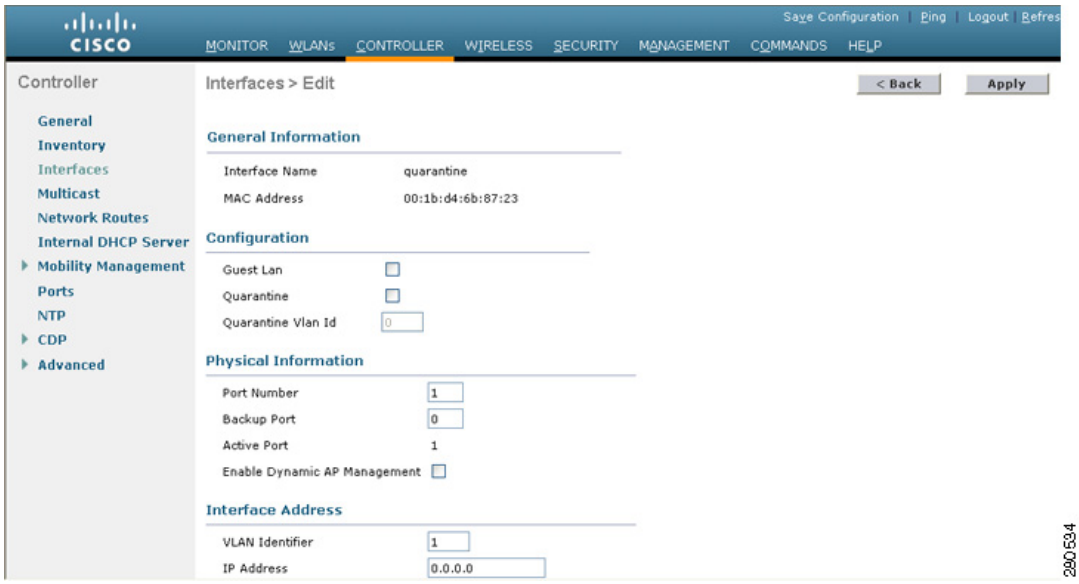
To create and specify settings for a new Dynamic Interface on the Wireless LAN Controller:

Step 1 In the WLC graphical user interface, click **Controller > Interfaces** to open the **Interfaces** page.

Step 2 Click **New** and enter an **Interface Name** and **VLAN ID** in the **Interfaces > New** page that appears.

Step 3 Click **Apply** to commit your changes. The **Interfaces > Edit** page appears (Figure 4-3).

Figure 4-3 WLC 4400 Interfaces > Edit Page



Step 4 Configure the following parameters:

- Guest LAN
- Enable the **Quarantine** option and specify a quarantine **Quarantine VLAN ID**.

Note Check the Quarantine check box if you want to configure this VLAN as unhealthy or you want to configure network access control (NAC) Out-of-Band integration. Doing so causes the data traffic of any client that is assigned to this VLAN to pass through the controller.

- Physical port assignment
- VLAN identifier
- Fixed IP address, IP netmask, and default gateway
- Primary and secondary DHCP servers
- Access control list (ACL) name, if required

Note To ensure proper operation, you must set the Port Number and Primary DHCP Server parameters.

Step 5 Click **Save Configuration** to save your changes.

Step 6 Repeat this procedure for each dynamic interface that you want to create or edit.

For more information, refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1*.

Create the WLAN on the Wireless LAN Controller and Enable Cisco NAC Appliance Integration

To create a new WLAN on the Wireless LAN Controller and enable integration with Cisco NAC Appliance:

Step 1 In the WLC graphical user interface, click **WLANs > New**. The **WLANs > New** page appears.

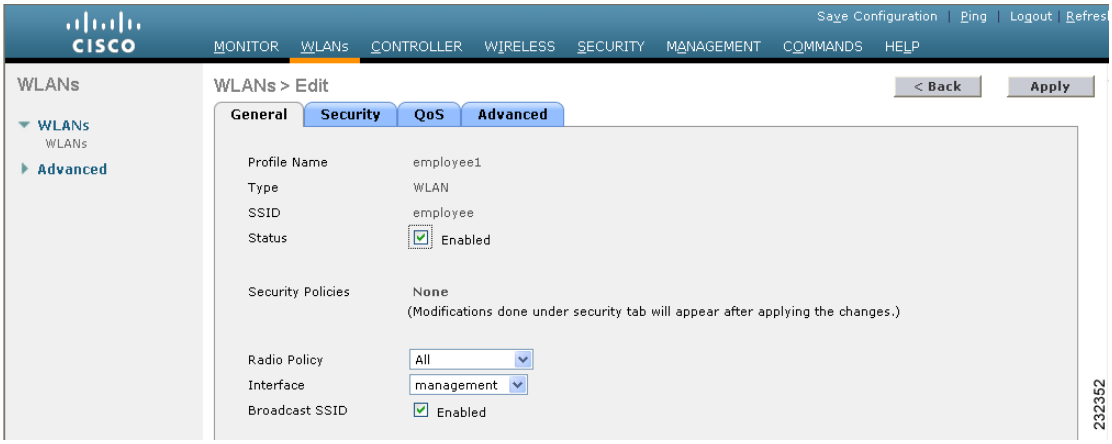
Step 2 Choose **WLAN** from the **Type** dropdown menu.

Step 3 Enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN in the **Profile Name** field. The profile name must be unique.

Step 4 Enter up to 32 alphanumeric characters for the SSID to be assigned to this WLAN in the **WLAN SSID** field.

Step 5 Click **Apply** to commit your changes. The **WLANs > Edit** page appears (Figure 4-4).

Figure 4-4 WLC 4400 WLANs > Edit Page



Step 6 On the **General** tab, check the **Status** checkbox to enable this WLAN.

Caution Leave this option *unchecked* (disabled) until you have finished making configuration changes to the WLAN.

Step 7 On the **Advanced** tab, check the State checkbox under the "NAC" heading to enable WLC integration with Cisco NAC Appliance.

Step 8 Specify a **Quarantine VLAN ID** for wireless user sessions when authenticating with Cisco NAC Appliance.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

For more information, refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1*.

Configure SNMP on the Wireless LAN Controller

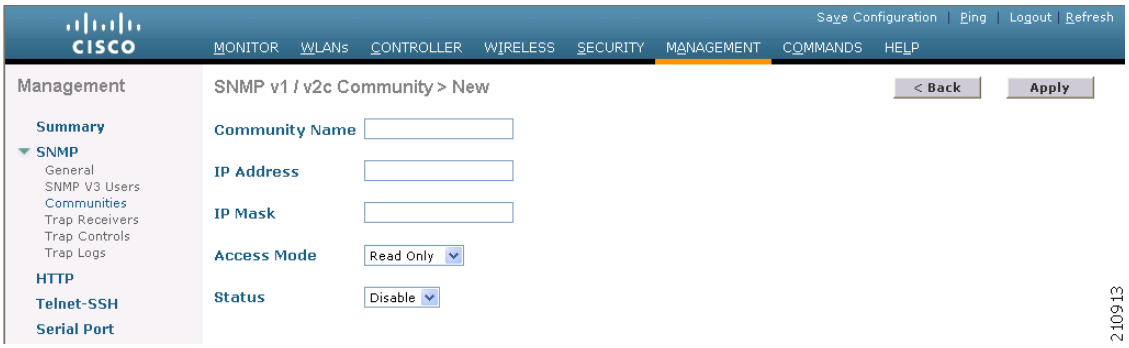
To ensure the Wireless LAN Controller is able to receive and process SNMP transmissions from the CAM regarding OOB client machine status in the Cisco NAC Appliance system, you must enable and configure SNMP behavior on the WLC.

To create a new SNMP community and enable SNMP on the WLC:

Step 1 Click **Management** and then **Communities** under SNMP. The **SNMP v1 / v2c Community** page appears.

Step 2 Click **New** to create a new community. The **SNMP v1 / v2c Community > New** page appears (Figure 4-5).

Figure 4-5 SNMP v1 / v2c Community > New Page



Step 3 In the **Community Name** field, enter a unique name containing up to 16 alphanumeric characters. (Do not enter "public" or "private.")

Step 4 Enter the **IP Address** of the CAM from which this device accepts SNMP packets with the associated community and the respective **IP Mask**.

Step 5 Choose **Read/Write** from the **Access Mode** dropdown menu to specify the access level for this community.

Step 6 Choose **Enable** from the **Status** dropdown menu to activate this community.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your settings.

Step 9 Repeat this procedure if a "public" or "private" community still appears on the **SNMP v1 / v2c Community** page.

For more information, refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1*.

Specify the CAM as the SNMP Trap Receiver

Once you enable and configure SNMP on the Wireless LAN Controller, you must also ensure the WLC knows which CAM is receiving SNMP trap messages.

To specify the host name and IP address of the SNMP trap receiver CAM:

Step 1 Click **Management** and then **Trap Receivers** under SNMP. The **SNMP Trap Receivers > New** page appears (Figure 4-6).

Figure 4-6 SNMP Trap Receivers > New Page



Step 2 Specify the host name of the CAM to receive SNMP traps from the WLC in the **Trap Receiver Name** field.

Step 3 Enter the CAM's IP address in the **IP Address** field.

Step 4 Choose **Enable** from the **Status** dropdown menu.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your settings.

Wireless OOB Network Setup/Configuration Worksheet

Table 4-3 summarizes information needed to configure WLCs and the Clean Access Manager.

Table 4-3 Configuration Worksheet

Configuration Settings	Value
Wireless LAN Controller Configuration	
WLC IP Address/Netmask:	
New dynamic interface	
SSID Access VLAN:	
SSID Authentication (Quarantine) VLAN:	
SNMP version used	
SNMP (V1/V2c) read community name:	
SNMP (V1/V2c) write community name:	
SNMP (V3) auth method/username/password:	
SNMP Trap V2c community string (to send traps to CAM):	
CAM/CAS Configuration	
CAM host name	
CAM IP address:	
CAS Trusted IP address:	
CAS Untrusted IP address:	
CAM SNMP Trap Receiver	
Community name for SNMP Trap V1 devices:	

Table 4-3 Configuration Worksheet (continued)

Configuration Settings	Value
Community name for SNMP Trap V2c devices:	
Auth method/username/password for SNMP Trap V3 WLCs:	

Configure Wireless LAN Controller Connection on the CAM

This section describes the web admin console configuration steps to implement Wireless OOB. In general, you first configure Group and Wireless LAN Controller profiles, and the CAM's SNMP Receiver settings under **OOB Management > Profiles**. After the WLC profile is configured, add the new WLC you want to communicate with to the Clean Access Manager's domain under **OOB Management > Devices**, and ensure the new profile appears in the Devices list.

The configuration sequence is as follows:

1. Plan your settings and configure the switches to be managed, as described in previous section, Configure Your Wireless LAN Controllers, page 4-7
2. Add a Wireless Out-of-Band Clean Access Server and Configure Environment, page 4-13
3. Configure Group Profiles, page 4-14
4. Configure Wireless LAN Controller Profiles, page 4-16
5. Configure SNMP Receiver, page 4-19
6. Add and Manage Wireless LAN Controllers, page 4-20

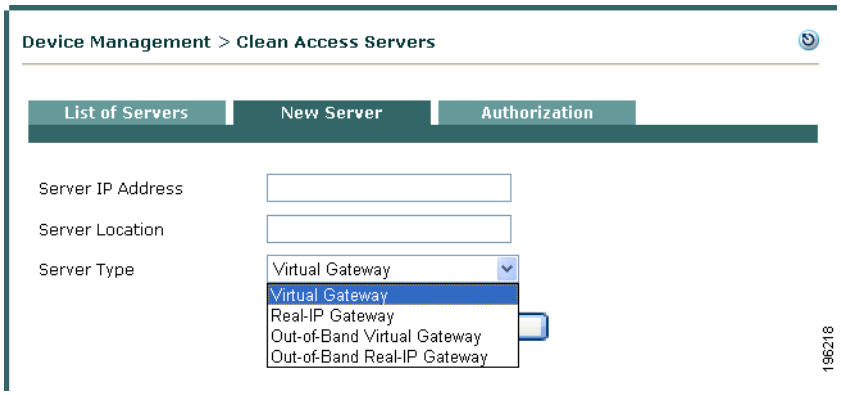
Add a Wireless Out-of-Band Clean Access Server and Configure Environment

Almost all the CAM/CAS configuration for Wireless Out-of-Band deployment is done directly in the **OOB Management** module of the CAM web console. If your Wireless LAN Controller installation features great enough throughput/bandwidth, you can (and may need to) configure more than one Clean Access Server to handle all of the authentication traffic between wireless client machines and the Cisco NAC Appliance system.

To add a Wireless OOB Clean Access Server to the CAM:

Step 1 Choose the **Out-of-Band Virtual Gateway** option from the **Server Type** dropdown menu (Figure 4-7).

Figure 4-7 Add New OOB Server



The Clean Access Server itself must be ***either*** In-Band or Out-of-Band. The Clean Access Manager can control both In-Band and Out-of-Band CASs in its domain.

Note You can only deploy CASs supporting wireless client machine authentication in Virtual Gateway mode.

Step 2 Enter the IP address of the Clean Access Server's eth0 (trusted) interface in the **Server IP Address** field.

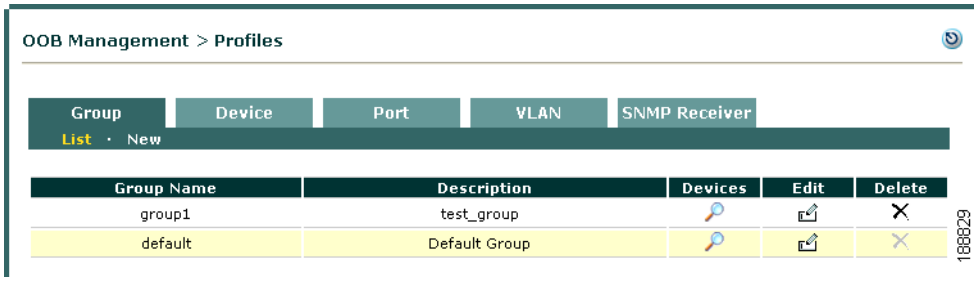
Step 3 (Optional) Enter the Clean Access Server location/description/purpose in the **Server Location** field.

Step 4 Click **Add Clean Access Server**.

Configure Group Profiles

When you first add a WLC to the Clean Access Manager's domain (under **OOB Management > Devices**), a Group profile must be applied to add the new WLC. There is a predefined Group profile called **default**, shown in Figure 4-8. All WLCs are automatically put in the **default** group when you add them. You can leave this default Group profile setting, or you can create additional Group profiles as needed. If you are adding and managing a large number of WLCs, creating multiple Group profiles allows you to filter which sets of devices to display from the list of WLCs (under **OOB Management > Devices > Devices > List**).

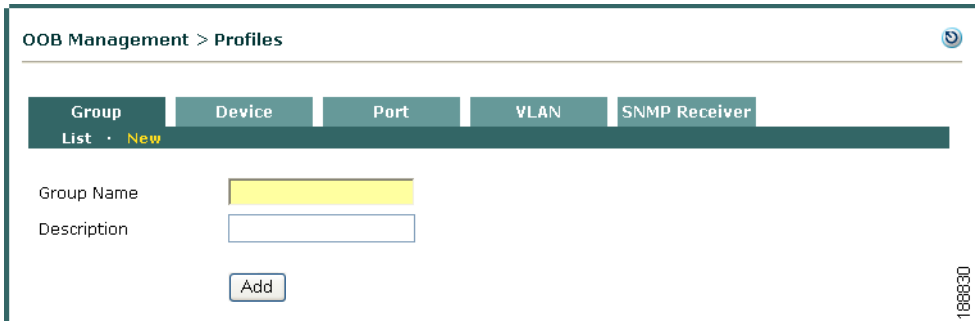
Figure 4-8 Group Profiles List



Add Group Profile

Step 1 Go to **OOB Management > Profiles > Group > New** (Figure 4-9).

Figure 4-9 New Group



Step 2 Enter a single word for the **Group Name**. You can use digits and underscores, but no spaces.

Step 3 Enter an optional **Description**.

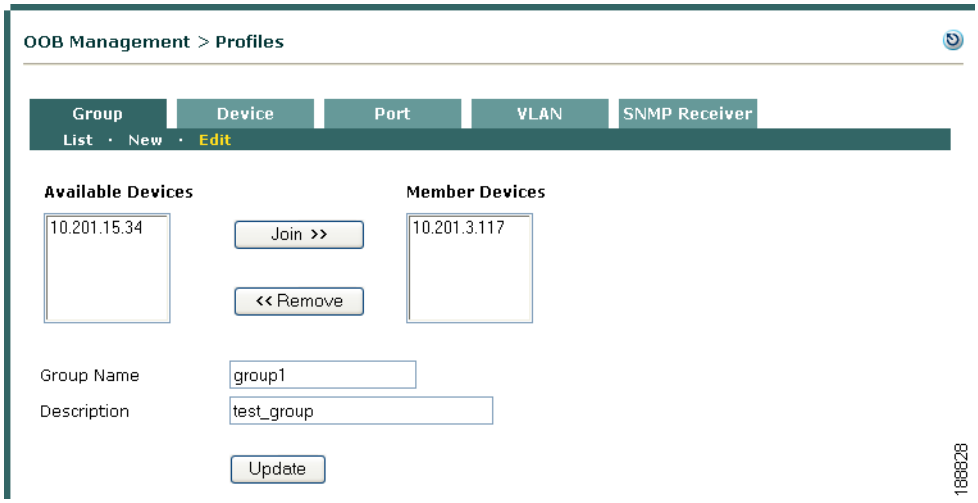
Step 4 Click **Add**. The new Group profile appears under **OOB Management > Profiles > Group > List**.

Edit Group Profile

Step 1 To edit the profile later, after actual WLCs are added, go to **OOB Management > Profiles > Group > List** and click the **Edit** icon for the new Group profile.

Step 2 The **Edit** page appears (Figure 4-10).

Figure 4-10 Edit Group



Step 3 You can toggle the WLCs that belong in the Group profile by selecting the IP address of the WLC from the **Member Devices** or **Available Devices** columns and clicking the **Join** or **Remove** buttons as applicable.

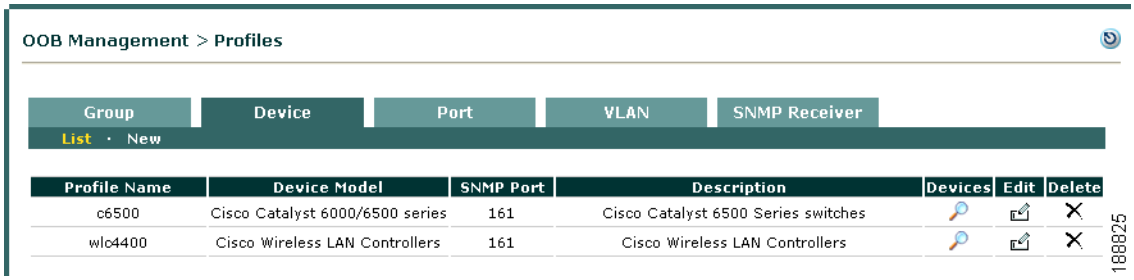
Step 4 Click the **Update** button when done to save your changes.

Note To delete a group profile, you must first remove the joined switches and/or WLCs from the profile.

Configure Wireless LAN Controller Profiles

A WLC profile must first be created under **OOB Management > Profiles > Device > New**, then applied when a new WLC is added. A WLC profile classifies WLCs of the same model and SNMP settings, as shown in Figure 4-11. The WLC profile configures how the CAM learns client Authentication/Access VLAN assignments from the WLC and when to remove Wireless OOB clients from the Online Users list for a WLC of that type.

Figure 4-11 Device Profiles List



The Device profiles list under **OOB Management > Profiles > Device > List** provides three icons:

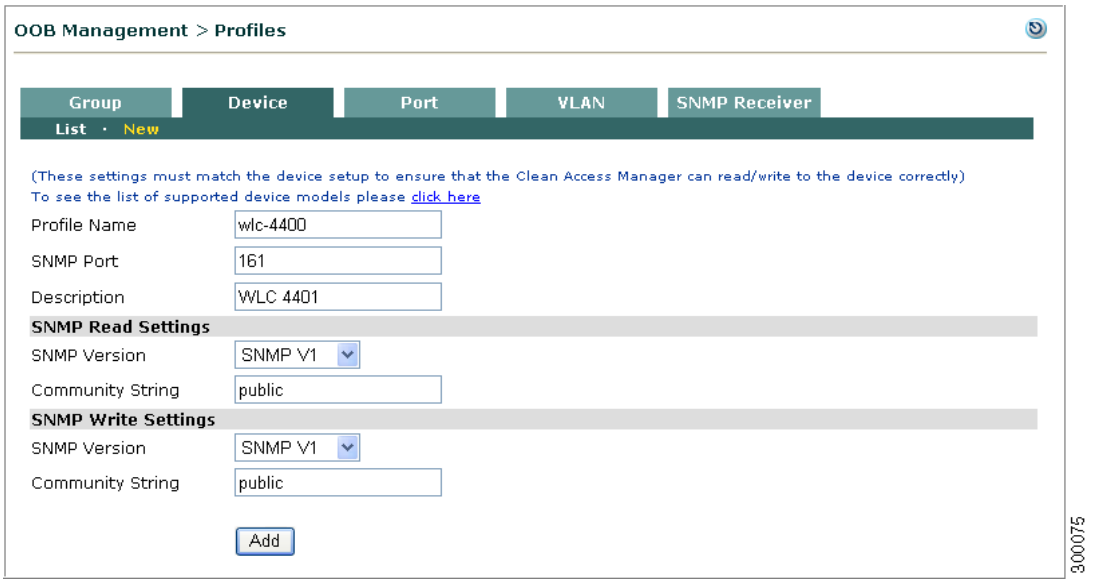
- **Devices**—Clicking this icon brings up the list of added devices under **OOB Management > Devices > Devices > List** (see Figure 4-15).
- **Edit**—Clicking this icon brings up the **Edit** Device profile form (see Figure 4-13).
- **Delete**—Clicking this icon deletes the Device profile (a confirmation dialog appears first).

Add Wireless LAN Controller Profile

Use the following steps to add a Wireless LAN Controller profile.

Step 1 Go to **OOB Management > Profiles > Device > New** (Figure 4-12).

Figure 4-12 New Wireless LAN Controller Profile



Step 2 Enter a single word for the **Profile Name**. You can use digits and underscores but no spaces.

Note It is a good idea to enter a WLC name that identifies the model and SNMP read and write versions, for example "WLC4400v2v3."

Step 3 Enter the **SNMP Port** configured on the WLC to receive read/write requests. The default port is 161 for SNMP GET/SET and the default port is 162 for Traps.

Step 4 Enter an optional **Description**.

Note You can click the link available at the top of this tab to view the list of supported device models.

Step 5 Configure **SNMP Read Settings** to match those on the WLC.

- Choose the **SNMP Version**: SNMP V1, SNMP V2C, or SNMP V3.
- Type the **Community String** for SNMP V1 or SNMP V2C configured for the WLC.

Step 6 If SNMP V3 is used for SNMP Read Settings on the WLC, configure the following settings to match those on the switch:

- Choose a **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES), or AuthPriv(SHA+DES).
- Type the **User Name**.
- Type the **User Auth**.
- Type the **User Priv**.

Step 7 Configure **SNMP Write Settings** to match those on the WLC.

- Choose the **SNMP Version**: SNMP V1, SNMP V2C, or SNMP V3.
- Type the **Community String** for SNMP V1 or SNMP V2C configured for the WLC.

Step 8 If SNMP v3 is used for SNMP write settings on the WLC, configure the following settings to match those on the WLC:

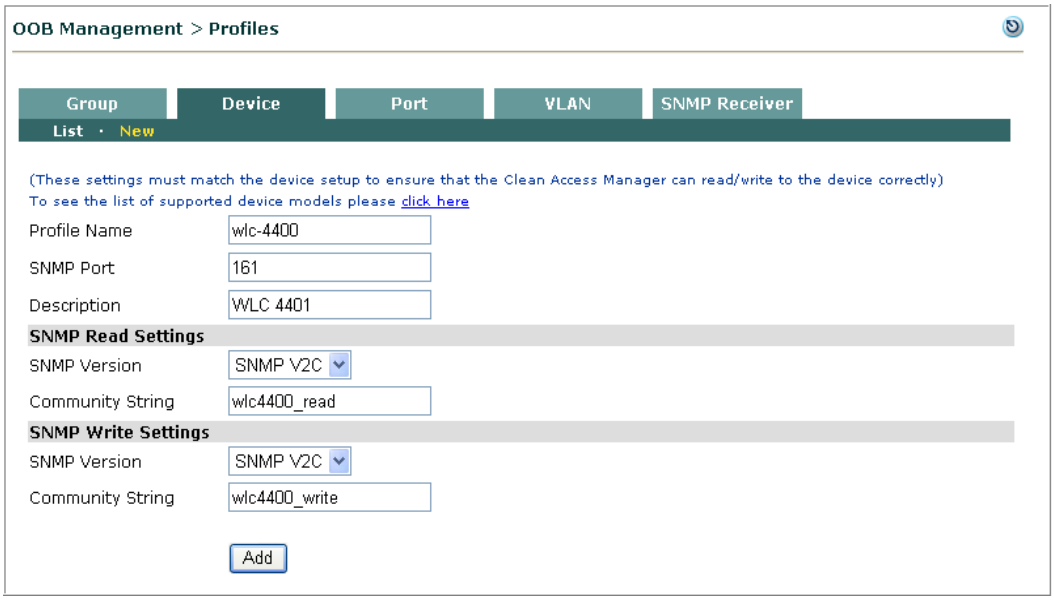
- Choose a **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES-CBC), or AuthPriv(SHA+DES-CBC).
- Type the **User Name.**
- Type the **User Auth.**
- Type the **User Priv.**

Note When WLC is rebooted, the SNMP V3 write may fail as the WLC SNMP engineboots value is not synced with CAM engineboots value. Each time you reboot WLC, update the switch profile. It is recommended to upgrade WLC to the latest version. For more details, refer to the caveat CSCtb78072 in *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.0.116.0*.

Step 9 Click **Add** to add the Wireless LAN Controller profile to **OOB Management > Profiles > Device > List** (Figure 4-15).

Figure 4-13 illustrates a WLC profile defining a Cisco 440 Wireless LAN Controller with the same SNMP settings: SNMP V2c with read community string "wlc4400_read" and write community string "wlc4400_write."

Figure 4-13 Example Wireless LAN Controller Profile



Configure SNMP Receiver

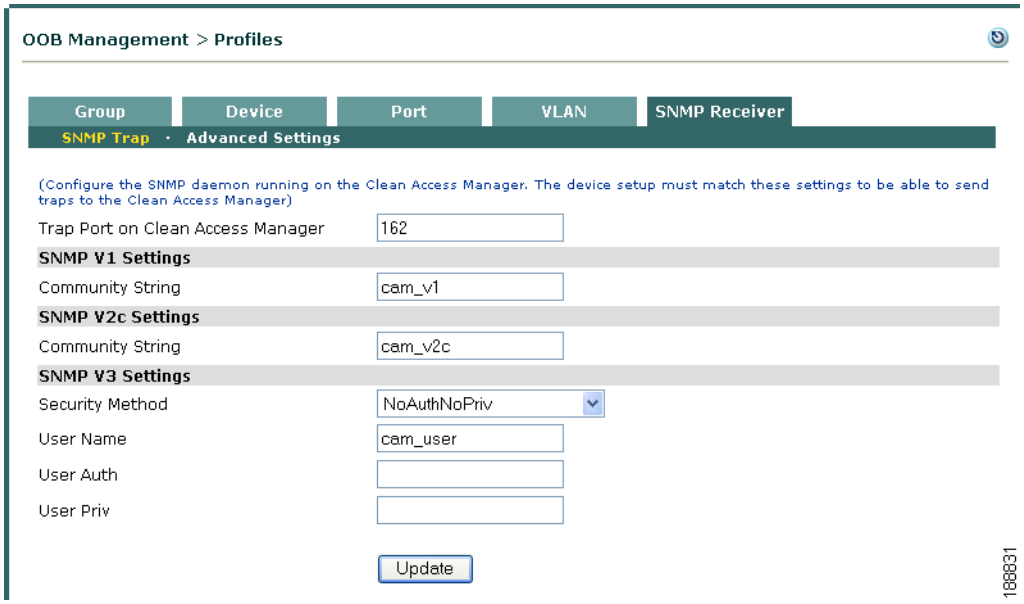
The **SNMP Receiver** form configures how the SNMP Receiver running on the Clean Access Manager receives and responds to SNMP trap notifications from WLCs when user events occur (such as when a user first logs on to or logs off of the network). The SNMP Receiver configuration on the CAM must match the WLC configuration in order for the WLC to send SNMP traps to the CAM.

SNMP Trap

This page configures settings for the SNMP traps the CAM receives from switches and WLCs. The Clean Access Manager SNMP Receiver can simultaneously support different versions of SNMP (V1, V2c, V3) when controlling groups of switches and/or WLCs in which individual devices may be using different versions of SNMP.

Step 1 Go to **OOB Management > Profiles > SNMP Receiver > SNMP Trap** (Figure 4-14).

Figure 4-14 CAM SNMP Receiver



Step 2 Use the default **Trap Port on Clean Access Manager** (162) or enter a new port number here.

Step 3 For **SNMP V1 Settings**, type the **Community String** used on switches using SNMP V1.

Step 4 For **SNMP V2c Settings**, type the **Community String** used on switches using SNMP V2c.

Step 5 For **SNMP V3 Settings**, configure the following fields used on switches using SNMP V3:

- Choose the **Security Method** from the dropdown menu: NoAuthNoPriv, AuthNoPriv(MD5), AuthNoPriv(SHA), AuthPriv(MD5+DES-CBC), or AuthPriv(SHA+DES-CBC)
- Type the **User Name**.
- Type the **User Auth.**
- Type the **User Priv**

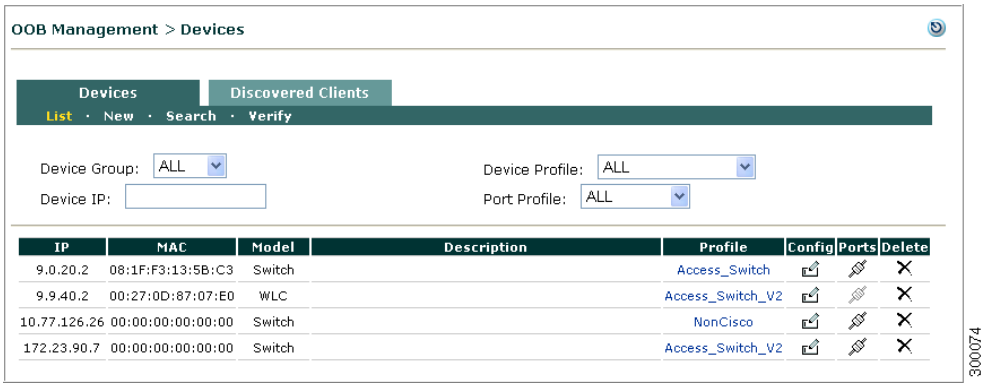
Step 6 Click **Update** to save settings.

Add and Manage Wireless LAN Controllers

The pages under the **OOB Management > Devices > Devices** tab are used to discover and add new switches and WLCs within an IP range, add new switches or WLCs by exact IP address, and manage the list of associated devices. There are two methods to add new managed WLCs:

- Add New Wireless LAN Controller, page 4-20
- Search New Wireless LAN Controllers, page 4-21
- Verify Devices, page 4-22

Figure 4-15 List of Devices



The list of devices under **OOB Management > Devices > Devices > List** displays all switches added from the **New** or **Search** forms. Wireless LAN Controller entries in the list include the WLC's IP address, MAC address, Description, and WLC Profile. You can sort the entries on the list by **Device Group** or **Device Profile** dropdowns, or you can simply type a **Device IP** and hit Enter to search for a switch by its address. Additionally the List provides one control and two icons:

- **Config**—Clicking the **Config** icon brings up the Config Tab, page 4-25 for the WLC.
- **Delete**—Clicking the **Delete** icon deletes the WLC from the list (a confirmation dialog appears before the WLC entry is removed).

Note The **Port Profile** dropdown is only used for adding switches to the Devices list and does not pertain to WLCs.

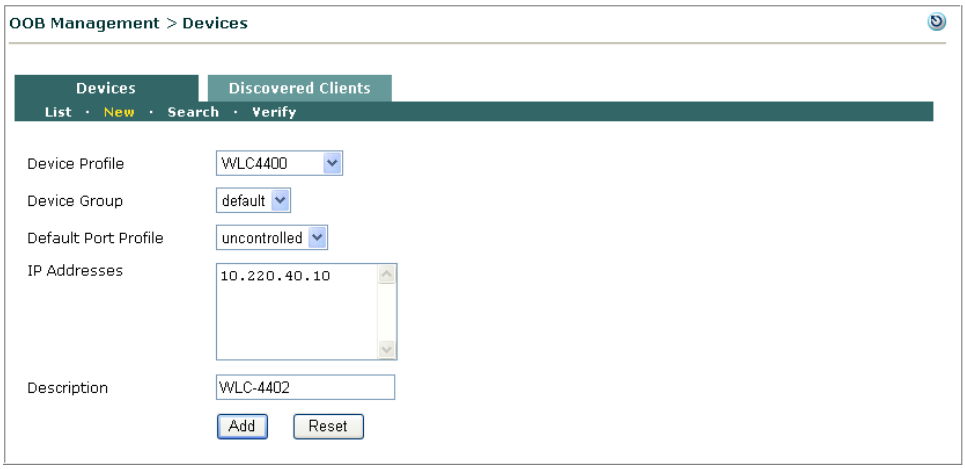
Profile links do not apply to WLCs and are "grayed out" in the Devices list for WLC entries.

Add New Wireless LAN Controller

The **New** page allows you to add WLCs when exact IP addresses are already known.

Step 1 Go to **OOB Management > Devices > Devices > New** (Figure 4-16).

Figure 4-16 Add New Wireless LAN Controller



Step 2 Choose the **Device Profile** from the dropdown menu to apply to the WLC to be added.

Step 3 Choose the **Device Group** for the WLC from the dropdown menu.

Step 4 Type the **IP Addresses** of the WLC(s) you want to add. Separate each IP address by line.

Step 5 Enter an optional **Description** of the new switch.

Step 6 Click the **Add** button to add the WLC(s).

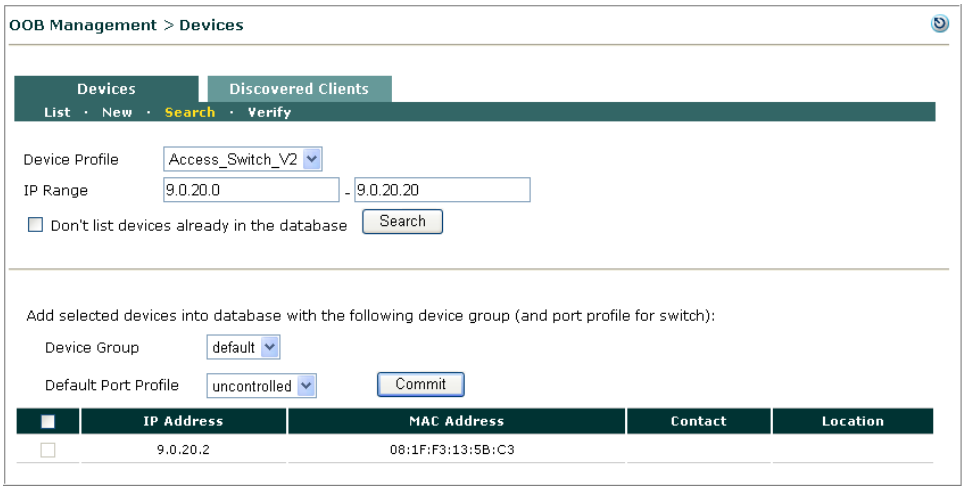
Step 7 Click the **Reset** button to reset the form.

Search New Wireless LAN Controllers

The **Search** page allows you to discover and add unmanaged switches within an IP range.

Step 1 Go to **OOB Management > Devices > Devices > Search** (Figure 4-17).

Figure 4-17 Search Devices



Step 2 Select a **Device Profile** from the dropdown list. The read community string of the selected WLC profile is used to find WLCs with matching read settings.

Step 3 Type an **IP Range** in the text box. (The maximum range for a search is 256 addresses.)

Step 4 By default, the **Don't list devices already in the database** checkbox is already checked. If you uncheck this box, the resulting search will include devices you have already added.

Step 5 Choose a **Device Group** from the dropdown to apply to the WLCs found in the search.

Step 6 Click the **checkbox** to the left of each WLC you want to connect with the CAM. Alternatively, click the checkbox at the top of the column to add *all* WLCs found from the search.

Note While all WLCs matching the read community string of the WLC profile used for the search are listed, only those WLCs matching the *read* SNMP version and community string can be added using the **Commit** button. The CAM cannot communicate with a WLC unless its *write* SNMP settings match those configured for its WLC profile.

Step 7 Click the **Commit** button to add the new devices. These devices are listed under **OOB Management > Devices > Devices > List**.

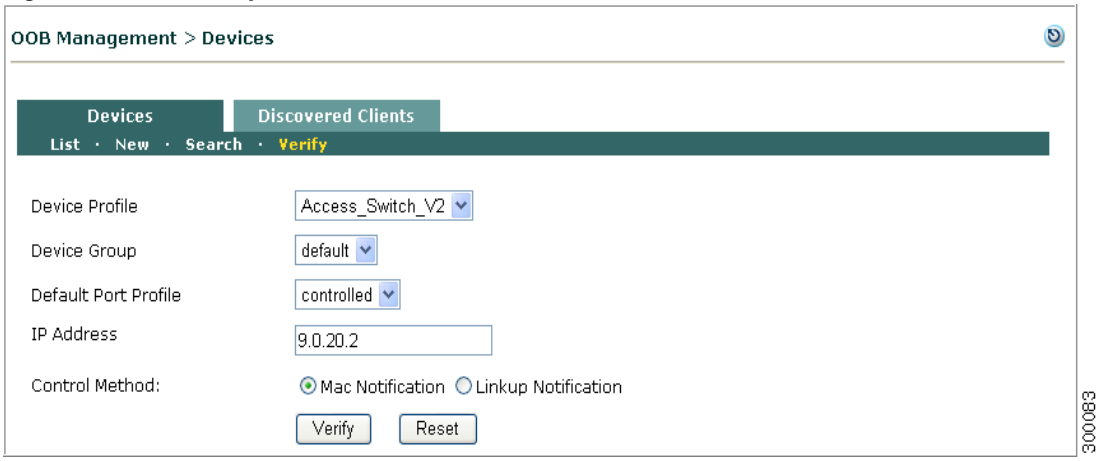
Verify Devices

The **Verify** page allows you to verify the devices. This utility verifies a device already added to CAM or a new device that is yet to be added to CAM. The device may be a switch or WLC.

Note Before verifying a device, ensure that you have setup the device profile and port profile, and configured the SNMP receiver for the device.

Step 1 Go to **OOB Management > Devices > Devices > Verify**.

Figure 4-18 Verify Devices



Step 2 Choose a **Device Profile** from the dropdown.

Step 3 Choose a **Device Group** from the dropdown.

Step 4 Choose a **Default Port Profile** from the dropdown.

Step 5 Type a valid **IP Address** in the text box.

Step 6 Choose the **Control Method** to configure the SNMP trap notification type that the CAM SNMP Receiver will use for a particular switch.

Note The **Control Method** is applicable only for the switches.

- **MAC Notification**—If a switch supports MAC Notification, choose this option.

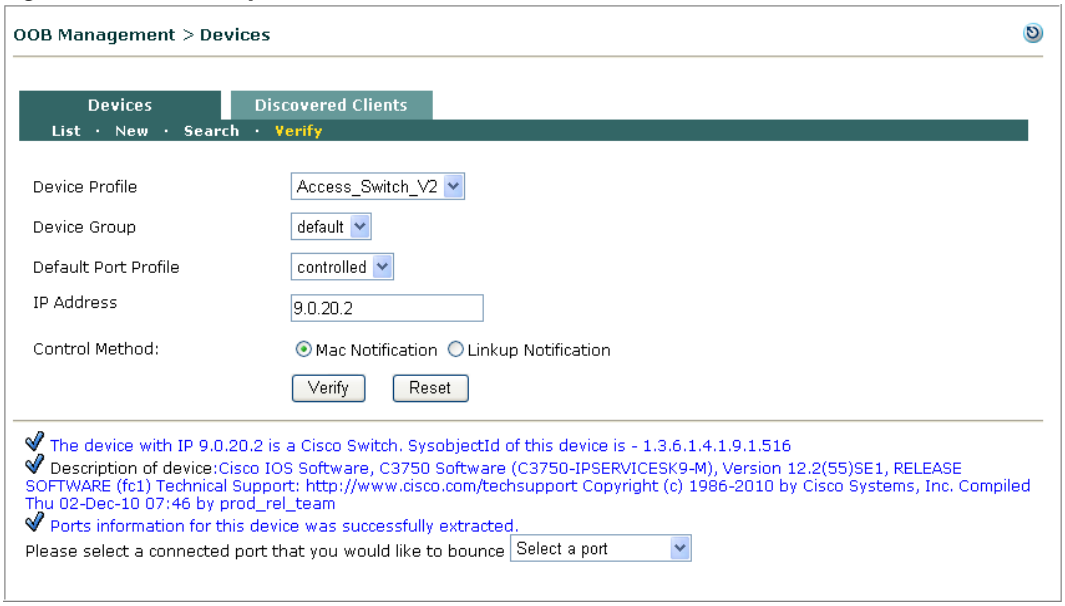
Note To support a variety of switch configurations, Cisco NAC Appliance supports switches using both MAC Change Notification and MAC Move Notification traps.

- **Linkup Notification**—If a switch does not support MAC Notification, then choose this option.

Step 7 Click **Verify**.

The device is verified and the results are displayed at the bottom of the page as shown in Figure 4-19.

Figure 4-19 Verify Devices - Result


OOB Management > Devices
Devices
Discovered Clients
List · New · Search · Verify
Device Profile
Access_Switch_V2
Device Group
default
Default Port Profile
controlled
IP Address
9.0.20.2
Control Method:
Mac Notification
Linkup Notification
Verify
Reset
The device with IP 9.0.20.2 is a Cisco Switch. SysobjectId of this device is - 1.3.6.1.4.1.9.1.516
Description of device:Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE1, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Thu 02-Dec-10 07:46 by prod_rel_team
Ports information for this device was successfully extracted.
Please select a connected port that you would like to bounce
Select a port
300084

The device status is displayed and you can select a connected port that you would like to bounce from the dropdown.

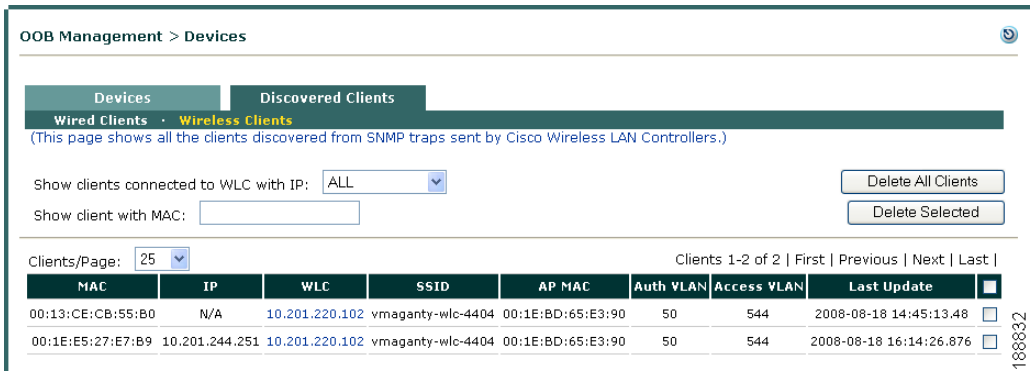
Discovered Wireless Clients

Figure 4-20 shows the **OOB Management > Devices > Discovered Clients > Wireless Clients** page. The Wireless Clients page lists all clients discovered by the Clean Access Manager via SNMP traps between the CAM and the WLC. The page records the activities of Out-of-Band clients (regardless of VLAN), based on the SNMP trap information that the Clean Access Manager receives.

When a client connects to a WLC and is assigned to the Authentication (Quarantine) VLAN, a trap is sent and the Clean Access Manager creates an entry on the Wireless Clients page. The Clean Access Manager adds a client's MAC address, IP address, associated WLC, Access Point MAC address, and Authentication (Quarantine) and Access VLAN assignments to the Wireless Clients list. Thereafter, the CAM updates the entry as it receives new SNMP trap information for the client.

Removing an entry from the Wireless Clients list clears this status information for the Wireless OOB client from the CAM.

Figure 4-20 Wireless Clients


OOB Management > Devices
Devices
Discovered Clients
Wired Clients · Wireless Clients
(This page shows all the clients discovered from SNMP traps sent by Cisco Wireless LAN Controllers.)
Show clients connected to WLC with IP: ALL
Show client with MAC:
Delete All Clients
Delete Selected
Clients/Page: 25
Clients 1-2 of 2 | First | Previous | Next | Last |
MAC IP WLC SSID AP MAC Auth VLAN Access VLAN Last Update
00:13:CE:CB:55:B0 N/A 10.201.220.102 vmaganty-wlc-4404 00:1E:BD:65:E3:90 50 544 2008-08-18 14:45:13.48
00:1E:E5:27:E7:B9 10.201.244.251 10.201.220.102 vmaganty-wlc-4404 00:1E:BD:65:E3:90 50 544 2008-08-18 16:14:26.876
188832

Elements of the page are as follows:

- **Show clients connected to WLC with IP**—Leave the default of ALL WLCs displayed, or choose a specific WLC from the dropdown menu. The dropdown menu displays all managed WLCs configured on the CAM.
- **Show client with MAC**—Type a specific MAC address and press Enter to display a particular client.
- **Clients/Page**—Leave the default of 25 entries displayed per page, or choose from the dropdown menu to displays 50, 100, 200, or ALL entries on the page.
- **Delete All Clients**—This button removes all clients on the list.
- **Delete Selected**—This button only removes the clients selected in the check column to the far right of the page.
- Note that you can click any of the following column headings to sort results by that column:
  - **MAC**—MAC address of discovered wireless client
  - **IP**—IP address of the wireless client
  - **WLC**—IP address of the originating Wireless LAN Controller. Clicking the WLC IP address brings up the **OOB Management > Devices > WLC [IP address] > Config > Basic** page for the WLC. (For more information, see Config Tab, page 4-25.)
  - **SSID**—The service set identifier to which the wireless client has been associated for network access.

- **AP MAC**—The MAC address of the WLC Access Point through which the client is accessing the network
- **Auth VLAN**—Authentication (Quarantine) VLAN
  A value of "N/A" in this column indicates that the VLAN ID for this MAC address is unavailable from the WLC.
- **Access VLAN**—Access VLAN of the client
  A value of "N/A" in this column indicates the Access VLAN ID is unavailable for the client. For example, if the user is switched to the Authentication VLAN but has never successfully logged into Cisco NAC Appliance (due to wrong user credentials), this machine will never have been assigned to the Access VLAN.
- **Last Update**—The last time the CAM updated the information of the entry.

See Wireless Out-of-Band Users, page 4-27 for additional details on monitoring Out-of-Band users.

Config Tab

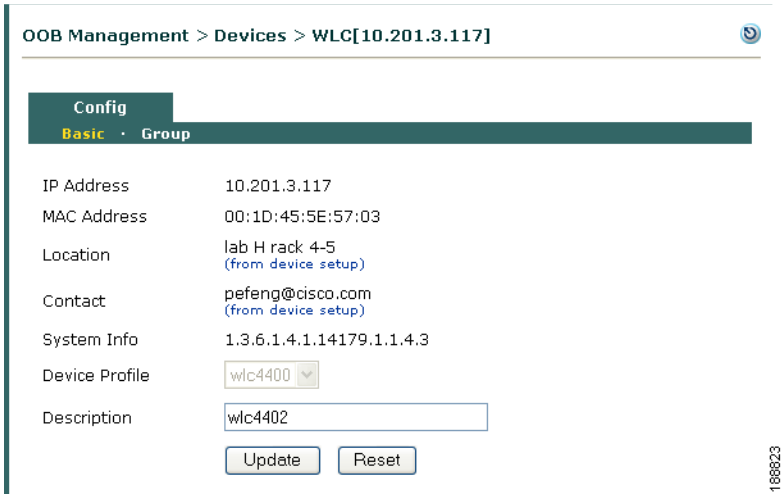
The Config tab allows you to modify Basic and Group profile settings for a particular Wireless LAN Controller:

- Basic
- Group

Basic

The Basic tab (Figure 4-21) shows the following values configured for the WLC.

Figure 4-21 Config > Basic



- The first values come from the initial configuration done on the WLC itself:
  - IP Address
  - MAC Address
  - Location
  - Contact
  - System Info (translated from the MIB for the WLC)

- **Device Profile**—Shows the Device Profile you are using for this WLC configured under **OOB Management > Profiles > Device**. The WLC Device Profile sets the model type, the SNMP port on which to send SNMP traps, SNMP version for read and write and corresponding community strings, or authentication parameters (SNMP V3 Write).
- **Description**—Optional description of the WLC. To change this field, type a new description and click **Update**.

Group

This page displays all the Group Profiles configured in the Clean Access Manager, and the Group Profiles to which the WLC currently belongs. You can add the WLC to other Groups, or you can remove the WLC from a Group Joined. To change the Group membership for all switches, go to **OOB Management > Profiles > Group** (see Configure Group Profiles, page 4-14).

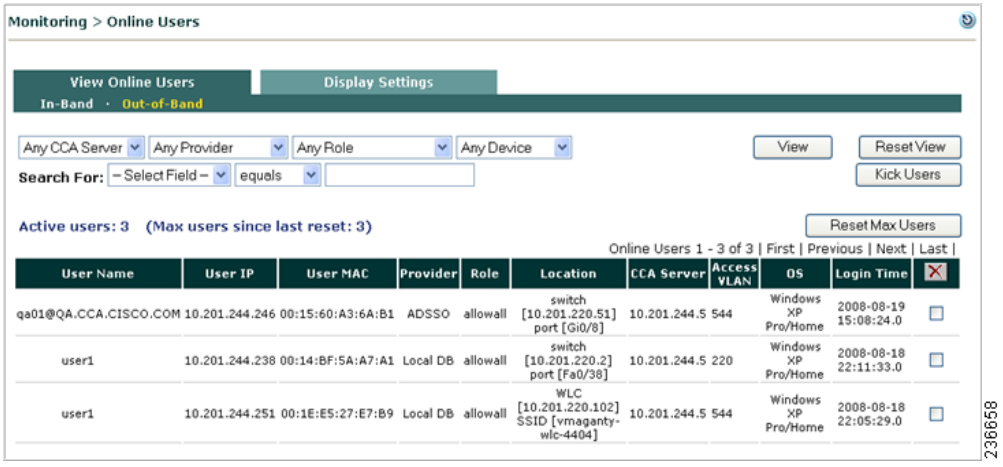
Figure 4-22 Config > Group



View Wireless Out-of-Band Online Users

When Out-of-Band is enabled, the **Monitoring > View Online Users** page displays links for both **In-Band** and **Out-of-Band** users and display settings (Figure 4-23). See Out-of-Band Users, page 11-31 for details.

Figure 4-23 View Out-of-Band Online Users


Monitoring > Online Users
View Online Users
Display Settings
In-Band · Out-of-Band
Any CCA Server
Any Provider
Any Role
Any Device
View
Reset View
Search For:
– Select Field –
equals
Kick Users
Active users: 3 (Max users since last reset: 3)
Reset Max Users
Online Users 1 - 3 of 3 | First | Previous | Next | Last |
User Name
User IP
User MAC
Provider
Role
Location
CCA Server
Access VLAN
OS
Login Time
qa01@QA.CCA.CISCO.COM 10.201.244.246 00:15:60:A3:6A:B1 ADSSO allowall switch [10.201.220.51] port [Gi0/8] 10.201.244.5 544 Windows XP Pro/Home 2008-08-19 15:08:24.0
user1 10.201.244.238 00:14:BF:5A:A7:A1 Local DB allowall switch [10.201.220.2] port [Fa0/38] 10.201.244.5 220 Windows XP Pro/Home 2008-08-18 22:11:33.0
user1 10.201.244.251 00:1E:E5:27:E7:B9 Local DB allowall WLC [10.201.220.102] SSID [vmaganty-wlc-4404] 10.201.244.5 544 Windows XP Pro/Home 2008-08-18 22:05:29.0
236658

Wireless Out-of-Band Users

Wireless OOB User Sessions

The following events trigger Wireless OOB users' disconnection from the Cisco NAC Appliance system:

- SNMP trap messages from the WLC
- Certified Timer expiration
- Session Timer expiration
- Manual removal from CAM

Following log-off, users must undergo authentication again before they are allowed back into the internal network. For additional details, see also Interpreting Event Logs, page 13-4 and Manage Certified Devices, page 11-10.

Note The change of VLAN configuration on CDL timer expiry is not supported for wireless OOB users.

Wireless and Wired OOB User List Summary

Table 3-4 on page 3-69 describes the lists used to track Out-of-Band users.



Configuring User Login Page and Guest Access

This chapter explains how to add the default login page needed for all users to authenticate and customize the login page for web login users. It also describes how to configure Guest User Access, page 5-17. Topics include:

- User Login Page, page 5-1
- Add Default Login Page, page 5-3
- Change Page Type (to Frame-Based or Small-Screen), page 5-4
- Enable Web Client for Login Page, page 5-5
- Customize Login Page Content, page 5-8
- Create Content for the Right Frame, page 5-11
- Upload a Resource File, page 5-13
- Customize Login Page Styles, page 5-14
- Configure Other Login Properties, page 5-15
- Guest User Access, page 5-17

For details on configuring the User Agreement Page for web login users, see Customize the User Agreement Page, page 12-19.

For details on configuring an Acceptable Use Policy page for Agent users, see Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 9-11.

For details on configuring user roles and local users, see Chapter 6, "User Management: Configuring User Roles and Local Users."

For details on configuring authentication servers, see Chapter 7, "User Management: Configuring Authentication Servers."

For details on configuring traffic policies for user roles, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

User Login Page

The login page is generated by Cisco NAC Appliance and shown to end users by role. When users first try to access the network from a web browser, an HTML login page appears prompting the users for a user name and password. Cisco NAC Appliance submits these credentials to the selected authentication provider, and uses them determine the role in which to put the user. You can customize this web login page to target the page to particular users based on a user's VLAN ID, subnet, and operating system.

Caution A login page must be added and present in the system in order for both web login and Agent users to authenticate. If a default login page is not present, Agent users will see an error dialog when attempting login ("Clean Access Server is not properly configured, please report to your administrator."). To quickly add a default login page, see Add Default Login Page, page 5-3.

Cisco NAC Appliance detects a number of client operating system types, including Windows, Mac OS X, Linux, Solaris, Unix, Palm, Windows CE, and others. Cisco NAC Appliance determines the OS the client is running from the OS identification in the HTTP GET request, the most reliable and scalable method. When a user makes a web request from a detected operating system, such as Windows XP, the CAS can respond with the page specifically adapted for the target OS.

When customizing the login page, you can use several styles:

- Frame-based login page (in which the login fields appear in a left-hand frame). This allows logos, files, or URLs to be referenced in the right frame of the page.
- Frameless login page (shown in Figure 5-6)
- Small screen frameless login page. The small page works well with Palm and Windows CE devices. The dimensions of the page are about 300 by 430 pixels.

Additionally, you can customize images, text, colors, and most other properties of the page.

This section describes how to add and customize the login page for all Clean Access Servers using the global forms of the Clean Access Manager. To override the global settings and customize a login page for a particular Clean Access Server, use the local configuration pages found under **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Login Page**. For further details, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Unauthenticated Role Traffic Policies

If a login page is customized to reference an external URL or server resource, a traffic policy must be created for the Unauthenticated role to allow users HTTP access to that URL or server. For details on configuring traffic policies for user roles, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

Note If Unauthenticated role policies are not configured to allow access to the elements referenced by the login page, or if a referenced web page becomes unavailable for some reason, you may see errors such as the login page continuing to redirect to itself after login credentials are submitted.

Proxy Settings

By default, the Clean Access Server redirects client traffic on ports 80 and 443 to the login page. If users on your untrusted network are required to use a proxy server and/or different ports, you can configure the CAS with corresponding proxy server information in order to appropriately redirect HTTP/HTTPS client traffic to the login page (for unauthenticated users) or HTTP/HTTPS/FTP traffic to allowed hosts (for quarantine or Temporary role users). You can specify:

- Proxy server ports only (for example, 8080, 8000)—this is useful in environments where users may go through a proxy server but not know its IP address (e.g. university).

- Proxy server IP address and port pair (for example, 10.10.10.2:80) — this is useful in environments where the IP and port of the proxy server to be used are known (e.g. corporate/enterprise).

Note Proxy settings are local policies configured on the CAS under **Device Management > Clean Access Servers > Manage [CAS_IP] > Advanced > Proxy**. For complete details, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

See also Proxy Servers and Host Policies, page 8-12 for related information.

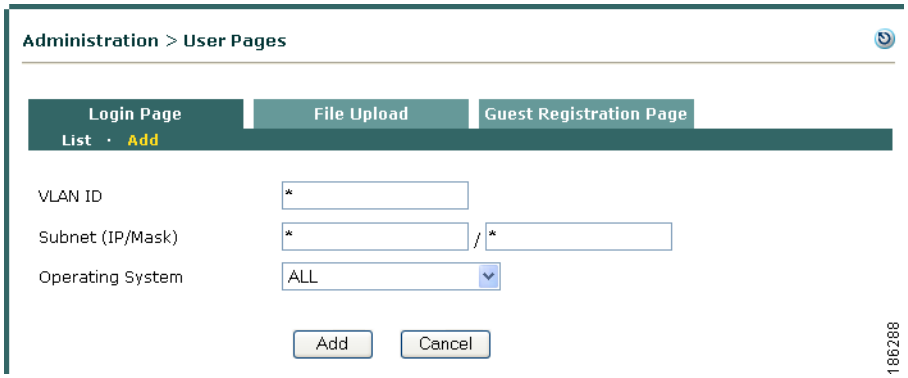
Add Default Login Page

A default login page must be added to the system to enable users to log in. For initial testing, you can follow the steps below leaving all default settings (*) to add a default login page. You can later define specialized login pages for target subnets and user operating systems. The following steps describe how to add a login page to the Clean Access Manager for all Clean Access Servers.

1. Go to **Administration > User Pages > Login Page**.
2. Click the **Add** submenu link.
3. Specify a **VLAN ID**, **Subnet (IP/Mask)**, or **Operating System** target for the page. To specify any VLAN ID or subnet, use an asterisk (*) in the field. For any OS, select **ALL**.

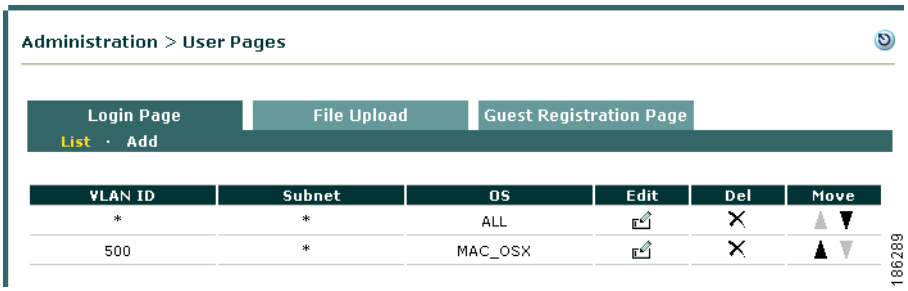
Note While choosing the Operating System, select MAC_OSX for Mac OS X client machines and select MAC_ALL for other devices like iPhones running iOS.

Figure 5-1 Add Login Page



4. Click **Add**.
5. The new page will appear under **Administration > User Pages > Login Page > List**.

Figure 5-2 Login Page List



After the login page is added, you must Edit it to configure all of its other properties. For details see:

- Change Page Type (to Frame-Based or Small-Screen), page 5-4
- Enable Web Client for Login Page, page 5-5
- Customize Login Page Content, page 5-8
- Create Content for the Right Frame, page 5-11
- Customize Login Page Styles, page 5-14
- Configure Other Login Properties, page 5-15

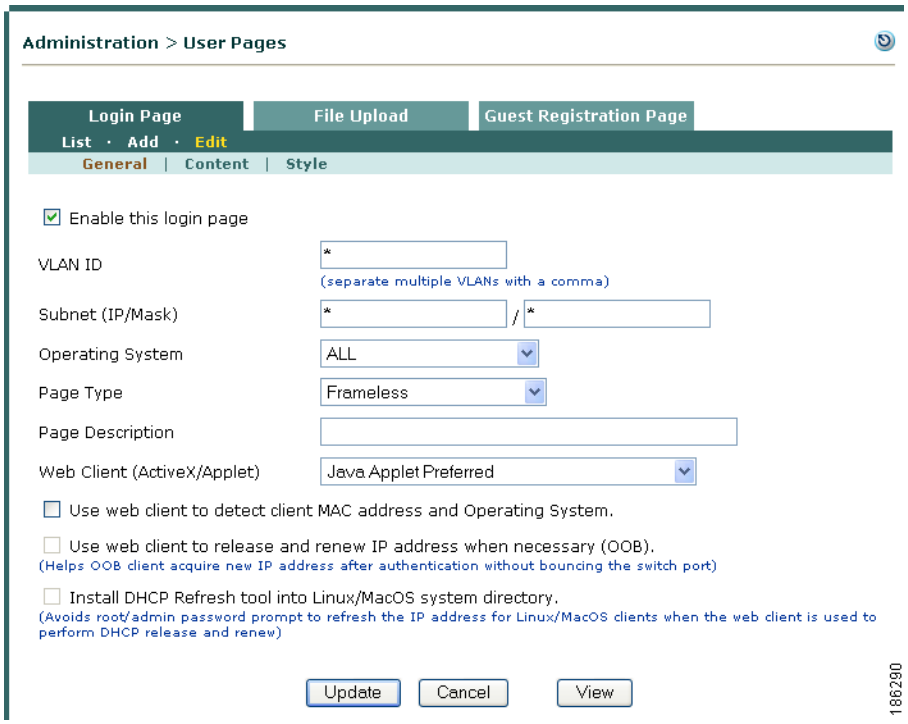
Change Page Type (to Frame-Based or Small-Screen)

After adding a login page, you edit its General properties to enable/disable it, change the target VLAN ID/ subnet or operating system, change the page type to frame-based or small screen, or enable the use of ActiveX/ Java Applet controls (see Enable Web Client for Login Page, page 5-5 for details).

To change the format of the page from the default frameless format, use the following steps:

1. From **Administration > User Pages > Login Page > List**, click the **Edit** icon next to the page to be customized.
2. The **General** subtab page appears by default.

Figure 5-3 General Login Page Properties—Configuring Page Type


Administration > User Pages
Login Page
File Upload
Guest Registration Page
List · Add · Edit
General | Content | Style
Enable this login page
VLAN ID
*
(separate multiple VLANs with a comma)
Subnet (IP/Mask)
* / *
Operating System
ALL
Page Type
Frameless
Page Description
Web Client (ActiveX/Applet)
Java Applet Preferred
Use web client to detect client MAC address and Operating System.
Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)
Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)
Update
Cancel
View
186290

3. From the **Page Type** dropdown menu, choose one of the following options:
   - **Frameless** (default)
   - **Frame-based**—This sets the login fields to appear in the left frame of the page, and allows you to configure the right frame with your own customized content (such as organizational logos, files, or referenced URLs). See Create Content for the Right Frame, page 5-11 for further details.
   - **Small Screen (frameless)**—This sets the login page as a small page works well with Palm and Windows CE devices. The dimensions of the page are about 300 by 430 pixels.
4. Leave other settings at their defaults.
5. Click **Update** to save your changes.

Enable Web Client for Login Page

The web client option can be enabled for all deployments but is required for L3 OOB.

To set up the Cisco NAC Appliance for L3 Out-of-Band (OOB) deployment, you must enable the login page to distribute either an ActiveX control or Java Applet to users who are multiple L3 hops away from the CAS. The ActiveX control/Java Applet is downloaded when the user performs web login and is used to obtain the correct MAC address of the client. In OOB deployment, the CAM needs the correct client MAC address to control the port according to Certified Devices List and/or device filter settings of the Port Profile.

Note When the Agent is installed, the Agent automatically sends the MAC address of all network adapters on the client to the CAS. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for more information.

DHCP Release/Renew with Agent/ActiveX/Java Applet

DHCP IP addresses can be refreshed for client machines using the Agent or ActiveX Control/Java Applet without requiring port bouncing after authentication and posture assessment. This feature is intended to facilitate Cisco NAC Appliance OOB deployment in IP phone environments.

In most OOB deployments (except L2 OOB Virtual Gateway where the Default Access VLAN is the Access VLAN in Port profile), the client needs to acquire a different IP address from the Access VLAN after posture assessment.

There are two approaches to enable the client to get the new IP address:

- Enabling the **Bounce the port after VLAN is changed** Port profile option. In this case, the switch port connected to the client is bounced after it is assigned to the Access VLAN, and the client using DHCP will try to refresh the IP address. This approach has the following limitations:
  - In IP phone deployments, because the port bouncing will disconnect and reconnect the IP Phone connected to the same switch port, any ongoing communication is interrupted.
  - Some client operating systems do not automatically refresh their DHCP IP addresses even if the switch port is bounced.
  - The process of shutting down and bringing back the switch port, and of client operating systems detecting the port bounce and refreshing their IP addresses can take time.
- Using the Agent, ActiveX Control, or Java Applet to refresh client DHCP IP addresses without port bouncing. This allows clients to acquire a new IP address in the Access VLAN and the **Bounce the switch port after VLAN is changed** option in the Port profile can be left disabled.

Note This option can introduce unpredictable results for OOB clients if not configured correctly for your specific network topology. For detailed information on Access to Authentication VLAN change detection, refer to Configure Access to Authentication VLAN Change Detection, page 3-67.

Agent Login

If the client uses the Agent to log in, the Agent automatically refreshes the DHCP IP address if the client needs a new IP address in the Access VLAN.

Web Login

In order for the ActiveX/Java Applet to refresh the IP address for the client when necessary, use of the web client must be enabled in the User Login Page configuration under:

- **Administration > User Pages > Login Page > Edit > General**
- **Device Management > CCA Servers > Authentication > Login Page > Edit > General**

In the Login Page configuration, two options need to be checked to use the ActiveX/Applet webclient to refresh the client's IP address:

- Use web client to detect client MAC address and Operating System
- Use web client to release and renew IP address when necessary (OOB)

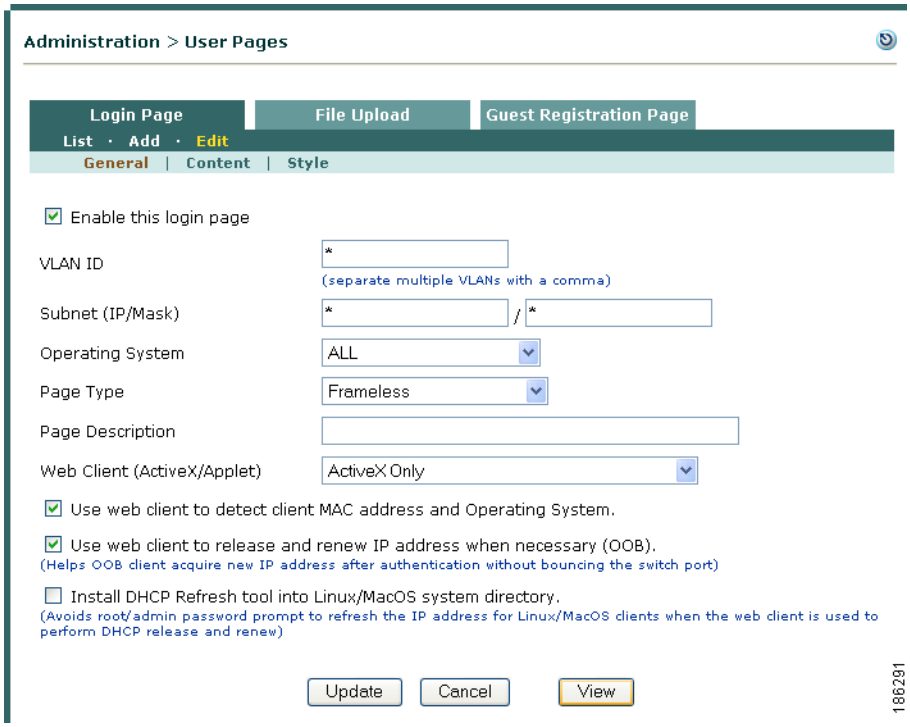
In the same configuration page, the network administrator can set the webclient preferences. Normally the Linux/Mac OS X clients are prompted for the root/admin password to refresh their IP address if the client user does not have the privilege to do so. To avoid the root/admin password prompt to refresh the IP address for Linux/Mac OS X clients, another option is used, the **Install DHCP Refresh tool into Linux/Mac OS system directory** option.

Note See Advanced Settings, page 3-45 for additional details on configuring DHCP Release, VLAN Change, and DHCP Renew Delays for OOB.

To enable the web client:

Step 1 Go to **Administration > User Pages > Login Page > Edit | General**.

Figure 5-4 Enable Web Client (ActiveX/Java Applet)


Administration > User Pages
Login Page
File Upload
Guest Registration Page
List · Add · Edit
General | Content | Style
Enable this login page
VLAN ID
*
(separate multiple VLANs with a comma)
Subnet (IP/Mask)
* / *
Operating System
ALL
Page Type
Frameless
Page Description
Web Client (ActiveX/Applet)
ActiveX Only
Use web client to detect client MAC address and Operating System.
Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)
Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)
Update
Cancel
View
186291

Step 2 From the **Web Client (ActiveX/Applet)** dropdown menu, choose one of the following options. For "Preferred" options, the preferred option is loaded first, and if it fails, the other option is loaded. With Internet Explorer, ActiveX is preferred because it runs faster than the Java Applet.

- **ActiveX Only**—Only runs ActiveX. If ActiveX fails, does not attempt to run Java Applet.
- **Java Applet Only**—Only runs Java Applet. If Java Applet fails, does not attempt to run ActiveX.
- **ActiveX Preferred**—Runs ActiveX first. If ActiveX fails, attempts to run Java Applet.
- **Java Applet Preferred**—Runs Java Applet first. If Java Applet fails, attempts to run ActiveX.

- **ActiveX on IE, Java Applet on non-IE Browser** (Default)—Runs ActiveX if Internet Explorer is detected, and runs Java Applet if another (non-IE) browser is detected. If ActiveX fails on IE, the CAS attempts to run a Java Applet. For non-IE browsers, only the Java Applet is run.

The following two options need to be checked to use the ActiveX/Java Applet web client to refresh the client's IP address:

Step 3 Click the checkbox for **Use web client to detect client MAC address and Operating System**.

Note For a Windows 8.1 client machine, while configuring the user pages in CAM web console, if you have selected the web client as 'Java Applet Only' and enabled the 'Use web client to detect client MAC address and Operating System' option, then the client Operating System might be detected as Windows 8. While using Applet for Windows 8.1, configure the user page with the operating system as **WINDOWS_ALL**.

Step 4 Click the checkbox for **Use web client to release and renew IP address when necessary (OOB)** to release/renew the IP address for the OOB client after authentication without bouncing the switch port.

Note This option can introduce unpredictable results for OOB clients if not configured correctly for your specific network topology. For detailed information on Access to Authentication VLAN change detection, refer to Configure Access to Authentication VLAN Change Detection, page 3-67.

Step 5 When use of the web client is enabled for IP address release/renew, for Linux/Mac OS X clients, you can optionally click the checkbox for **Install DHCP Refresh tool into Linux/Mac OS system directory**. This will install a DHCP refresh tool on the client to avoid the root/admin password prompt when the IP address is refreshed.

Step 6 Click **Update** to save settings.

Note To use this feature. "Enable L3 support" must be enabled under **Device Management > CCA Servers > Manage[CAS_IP] > Network > IP**.

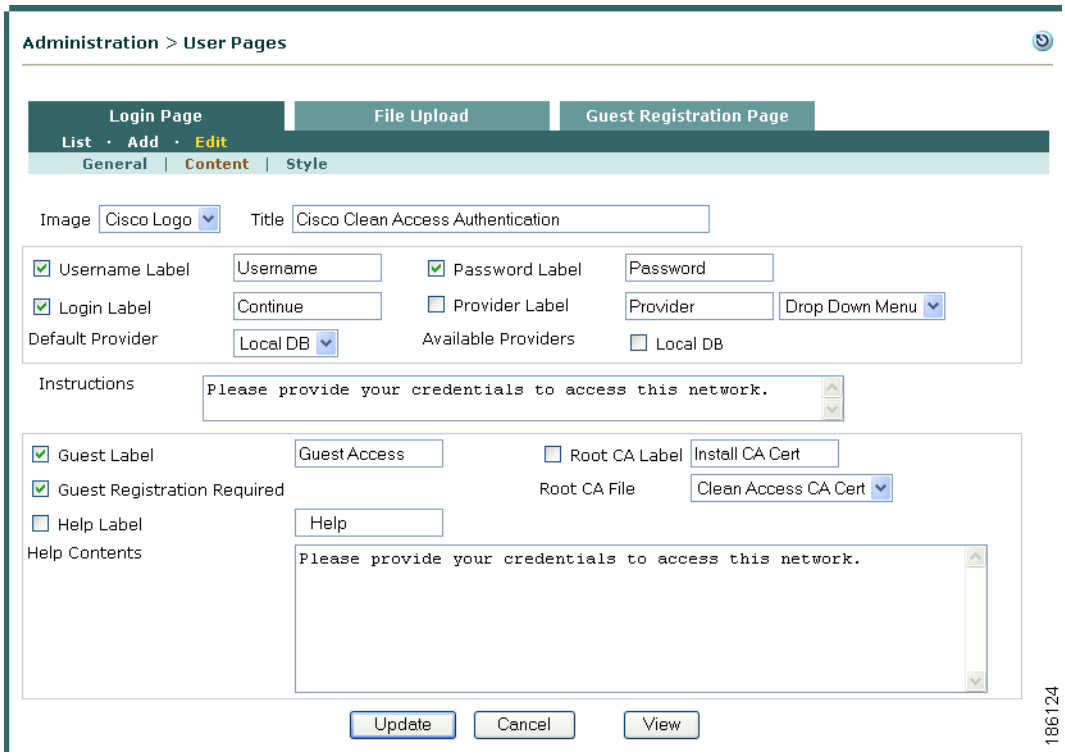
For further details, see "Configuring Layer 3 Out-of Band (L3 OOB) in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Customize Login Page Content

After adding a login page, you can edit the content that appears on the page.

1. From **Administration > User Pages > Login Page > List**, click the **Edit** icon next to the page to be customized.
2. Click the **Content** submenu link. The Login Page **Content** form appears.

Figure 5-5 Login Page Content



3. Configure the login page controls on the page using the following text fields and options.
   - **Image** – An image file, such as a logo, that you want to appear on the login page. To refer to your own logo, first upload the logo image. See Upload a Resource File, page 5-13.
   - **Title** – The title of the page as it will appear in the title bar of the browser window and above the login field.
   - **Username Label** – The label for the username input field.
   - **Password Label** – The label for the password input field.
   - **Login Label** – The label of the button for submitting login credentials.
   - **Provider Label** – The label beside the dropdown list of authentication providers.
   - **Default Provider** – The default provider presented to users.
   - **Available Providers** – Use the checkboxes to specify the authentication sources to be available from the **Providers** options on the login page. If neither the Provider Label nor these options are selected, the Provider menu does not appear on the login page and the Default Provider is used. Use the associated menu to specify the presentation method for users—either a dropdown menu containing the collection of selected providers or a collection of radio buttons the user can choose from.

Note Guest users accessing the Cisco NAC Appliance system via the preset "Guest" user account (described in Enable the Preset "Guest" User Account, page 5-22) must use the "Local DB" provider option.

If you are using the Guest User Registration feature, you must first configure a Guest provider type (described in Guest, page 7-26) and enable that provider type here to enable the Guest User Registration feature.

- **Instructions** – The informational message that appears to the user below the login fields. (This field accepts text-only entries. Do not use this field to enter HTML code and/or image file locations to display in the customized login page.)
- **Guest Label** – Determines whether a guest access button appears on the page with the text in the associated field as its label. This option serves two functions:

  This option allows users who do not have a login account to access the network as guest users per the guidelines in Enable the Preset "Guest" User Account, page 5-22.

  In conjunction with the **Guest Registration Required** option (below), this option enables users to log into the Cisco NAC Appliance system providing personalized credentials for individual guest users.

  Note Guest users accessing the Cisco NAC Appliance system via the preset "Guest" user account (described in Enable the Preset "Guest" User Account, page 5-22) must use the "Local DB" provider option.

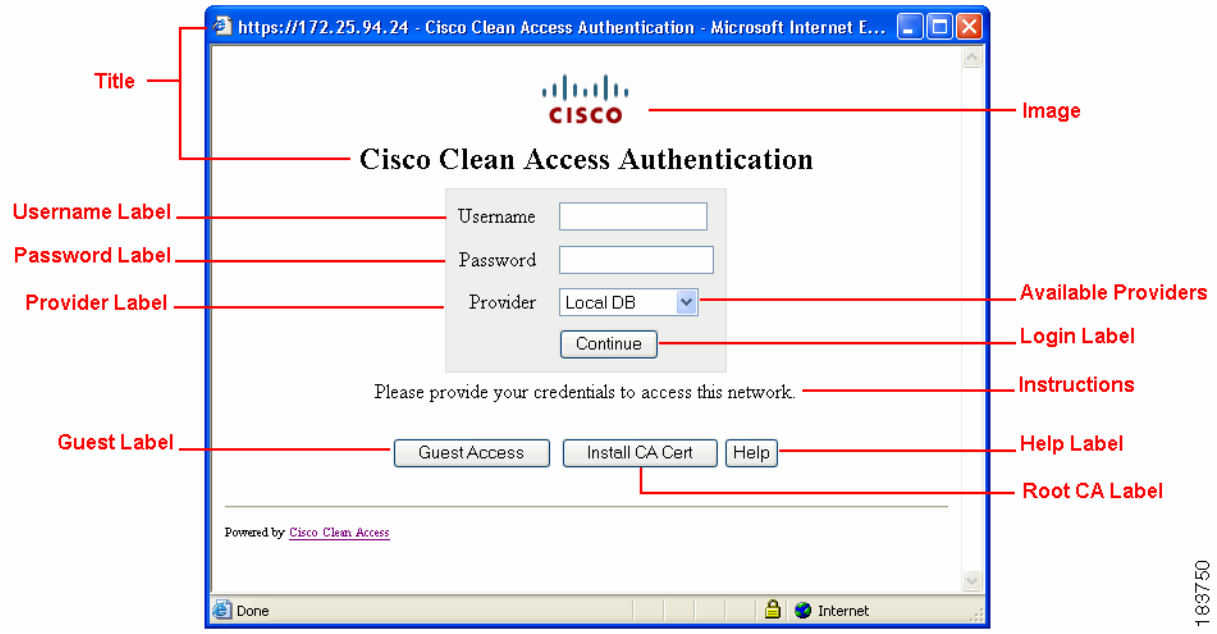
- **Guest Registration Required** – Enables the guest registration function that allows users to log in to the Cisco NAC Appliance system by specifying their user ID and affiliation in the guest login credentials screen. Turning on this option enables the guest user login and registration framework described in Configure Guest User Registration, page 5-17.

  Note You must enable both the **Guest Label** and **Guest Registration Required** options to use the Guest User Registration feature on the Cisco NAC Appliance system.

- **Help Label** – Determines if a help button appears on the page, along with its label.
- **Help Contents** – The text of the popup help window, if a help button is enabled. Note that only HTML content can be entered in this field (URLs cannot be referenced).
- **Root CA Label** – Places a button on the page users can click to install the root CA certificate file. When installed, the user does not have to explicitly accept the certificate when accessing the network.
- **Root CA File** – The root CA certificate file to use.

4. Click **Update** to save your changes.
5. After you save your changes, click **View** to see how your customized page will appear to users. Figure 5-6 illustrates how each field correlates to elements of the generated login page.

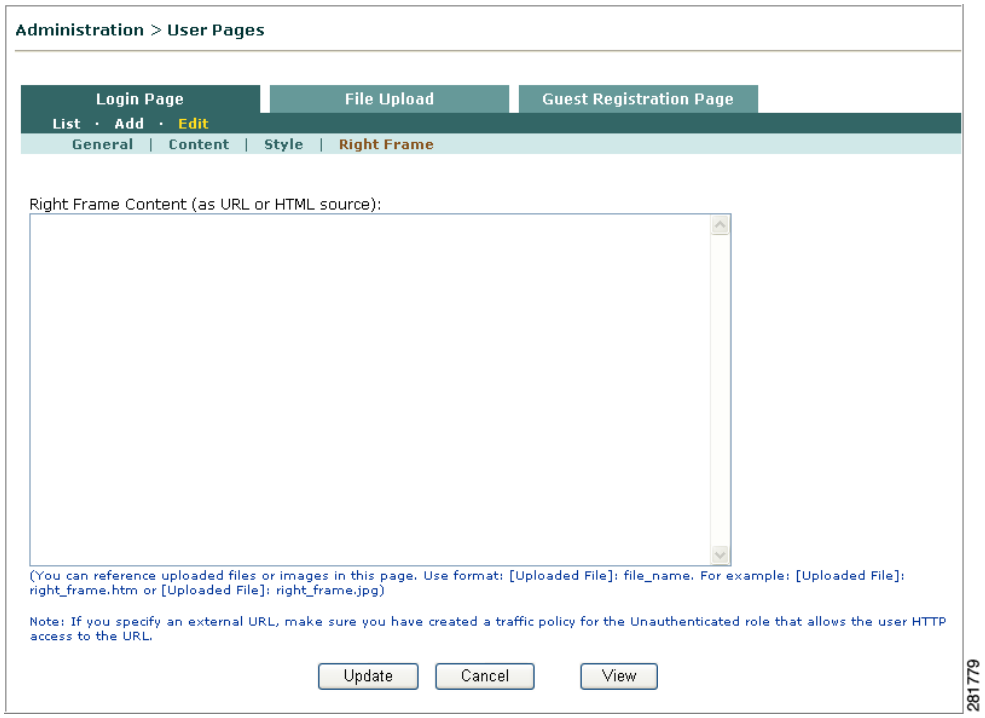
Figure 5-6 Login Page Elements



Create Content for the Right Frame

1. From **Administration > User Pages > Login Page > List**, click the **Edit** icon next to the page to be customized. If you have set the login page to be frame-based (as described in Change Page Type (to Frame-Based or Small-Screen), page 5-4), and additional **Right Frame** submenu link will appear for the page.
2. In the **Edit** form, click **Right Frame** sublink bring up the **Right Frame Content** form (Figure 5-7).

Figure 5-7 Login Page—Right Frame Content


Administration > User Pages
Login Page
File Upload
Guest Registration Page
List · Add · Edit
General | Content | Style | Right Frame
Right Frame Content (as URL or HTML source):
(You can reference uploaded files or images in this page. Use format: [Uploaded File]: file_name. For example: [Uploaded File]: right_frame.htm or [Uploaded File]: right_frame.jpg)
Note: If you specify an external URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access to the URL.
Update
Cancel
View
281779

3. You can enter a URL or HTML content for the right frame:

   a. ***Enter URL:*** (for a single webpage to appear in the right frame)

      For an external URL, use the format **`http://www.webpage.com`**.

      For a URL on the Clean Access Manager, use the format:

      `[Uploaded File]:file_name.htm`

      For images, use the format:

      `[Uploaded File]:file_name.jpg`

Note If you specify an external URL or Clean Access Manager URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access to the CAM or external server. In addition, if you change or update the external URLs referenced by the login page, make sure to update the Unauthenticated role policies as well. See Unauthenticated Role Traffic Policies, page 5-2 and Adding Traffic Policies for Default Roles, page 8-27 for details.

   b. ***Enter HTML:*** (to add a combination of resource files, such as logos and HTML links)

      Type HTML content directly into the **Right Frame Content** field.

      To reference any resource file you have already uploaded in the **File Upload** tab as part of the HTML content (including images, JavaScript files, and CSS files) use the following formats:

      To reference a link to an uploaded HTML file:

      ```
      <a href="file_name.html"> file_name.html </a>
      ```

      To reference an image file (such as a JPEG file) enter:

      ```
      <img src="file_name.jpg">
      ```

See also Upload a Resource File, page 5-13 for details.

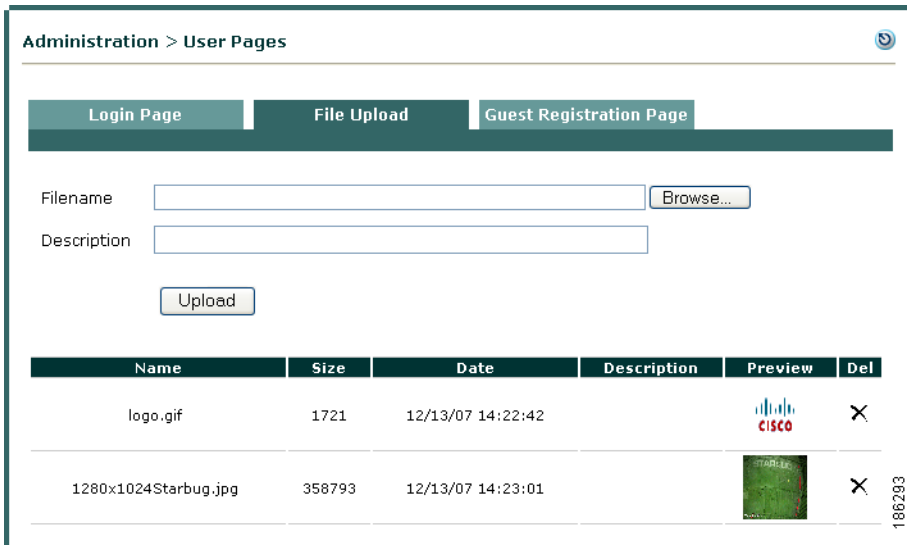
4. Click **Update** to save your changes.
5. After you save your changes, click **View** to see how your customized page will appear to users.

Upload a Resource File

Use the following steps to add a resource file, such as a logo for the **Image** field in the **Content** form or to add resources for a frame-based login page such as HTML pages, images, logos, JavaScript files, and CSS files. You can upload files that are up to 10MB in size.

Step 1 Go to **Administration > User Pages > File Upload**.

Figure 5-8 File Upload



Step 2 Browse to a logo image file or other resource file from your PC and select it in the **Filename** field.

Step 3 Optionally enter text in the **Description** field.

Step 4 Click **Upload**. The file should appear in the resources list.

Note

- Files uploaded to the Clean Access Manager using **Administration > User Pages > File Upload** are available to the Clean Access Manager and all Clean Access Servers. These files are located under `/perfigo/control/data/upload` in the CAM.
- Files uploaded to the CAM prior to 3.6(2)+ are not removed and continue to be located under `/perfigo/control/tomcat/normal-webapps/admin`.
- Files uploaded to a specific Clean Access Server using **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Login Page > File Upload** are available to the Clean Access Manager and the local Clean Access Server only. On the Clean Access Server, uploaded files are located under `/perfigo/access/tomcat/webapps/auth`. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for further information.

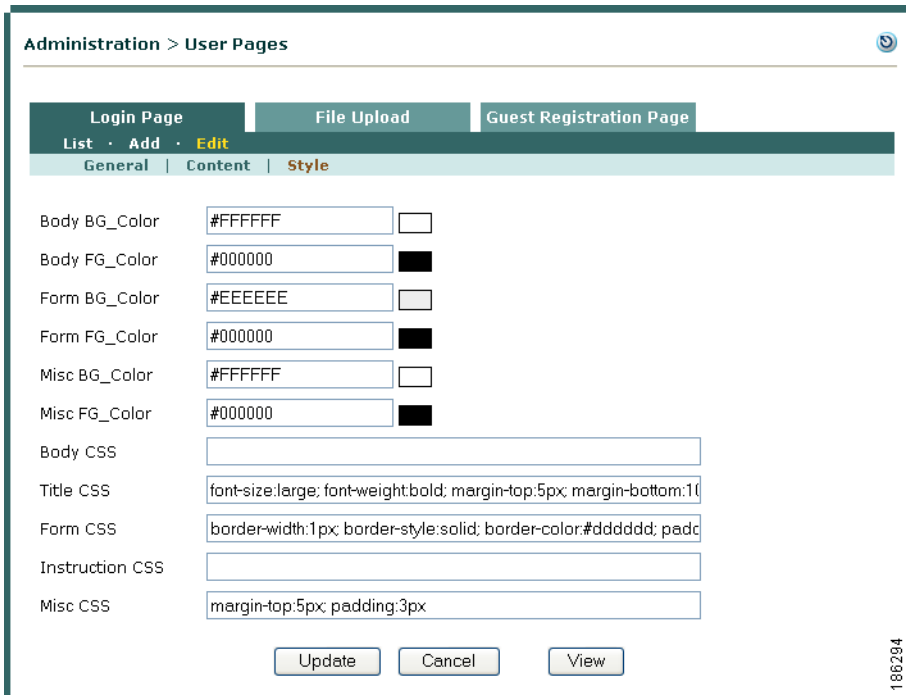
For further details on uploading content for the User Agreement Page (for web login/network scanning users), see also Customize the User Agreement Page, page 12-19.

For details on configuring traffic policies to allow client access to files stored on the CAM, see Adding Traffic Policies for Default Roles, page 8-27.

Customize Login Page Styles

1. Go to **Login Page > Edit > Style** to modify the CSS properties of the page.

Figure 5-9 Login Page Style



2. You can change the background (BG) and foreground (FG) colors and properties. Note that **Form** properties apply to the portion of the page containing the login fields (shaded gray in Figure 5-6 on page 5-11).
   - Left Frame Width: Width of the left frame contain login fields.
   - Body BG_Color, Body FG_Color: Background and foreground colors for body areas of the login page.
   - Form BG_Color, Form FG_Color: Background and foreground colors for form areas.
   - Misc BG_Color, Misc FG_Color: Background and foreground colors for miscellaneous areas of the login page.
   - Body CSS: CSS tags for formatting body areas of the login page.
   - Title CSS: CSS tags for formatting title areas of the login page.
   - Form CSS: CSS tags for formatting form areas of the login page.

- Instruction CSS: CSS tags for formatting instruction areas of the login page.
- Misc CSS: CSS tags for formatting miscellaneous areas of the login page.

3. Click **Update** to commit the changes made on the Style page, then click **View** to view the login page using the updated changes.

Configure Other Login Properties

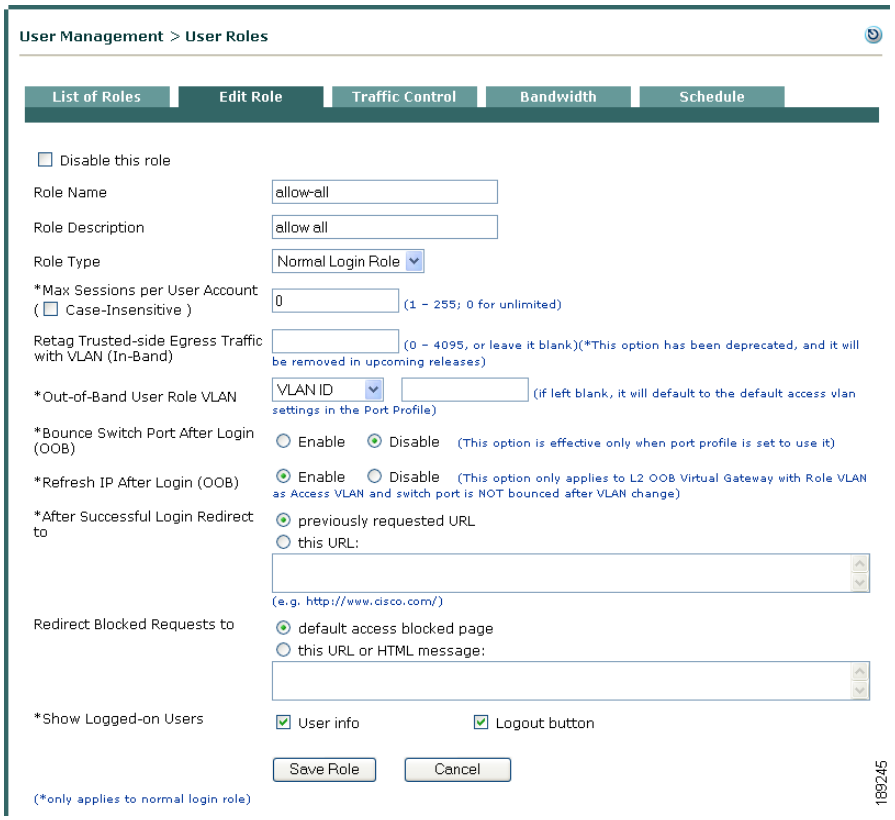
- Redirect the Login Success Page, page 5-15
- Specify Logout Page Information, page 5-16

Redirect the Login Success Page

By default, the CAM takes web login users who are authenticated to the originally requested page. You can specify another destination for authenticated users by role. To set the redirection target:

1. Go to **User Management > User Roles > List of Roles**.
2. Click the **Edit** icon next to the role for which you want to set a login success page (Figure 5-10).

Figure 5-10 Edit User Role Page


User Management > User Roles
List of Roles
Edit Role
Traffic Control
Bandwidth
Schedule
Disable this role
Role Name
allow-all
Role Description
allow all
Role Type
Normal Login Role
*Max Sessions per User Account
(Case-Insensitive)
0
(1 – 255; 0 for unlimited)
Retag Trusted-side Egress Traffic with VLAN (In-Band)
(0 – 4095, or leave it blank)(*This option has been deprecated, and it will be removed in upcoming releases)
*Out-of-Band User Role VLAN
VLAN ID
(if left blank, it will default to the default access vlan settings in the Port Profile)
*Bounce Switch Port After Login (OOB)
Enable
Disable
(This option is effective only when port profile is set to use it)
*Refresh IP After Login (OOB)
Enable
Disable
(This option only applies to L2 OOB Virtual Gateway with Role VLAN as Access VLAN and switch port is NOT bounced after VLAN change)
*After Successful Login Redirect to
previously requested URL
this URL:
(e.g. http://www.cisco.com/)
Redirect Blocked Requests to
default access blocked page
this URL or HTML message:
*Show Logged-on Users
User info
Logout button
Save Role
Cancel
(*only applies to normal login role)
189245

3. For the **After Successful Login Redirect to** option, click "**this URL"** and type the destination URL in the text field, making sure to specify "**http://**" in the URL. Make sure you have created a traffic policy for the role to allow HTTP access so that the user can get to the web page (see Add Global IP-Based Traffic Policies, page 8-4).
4. Click **Save Role** when done.

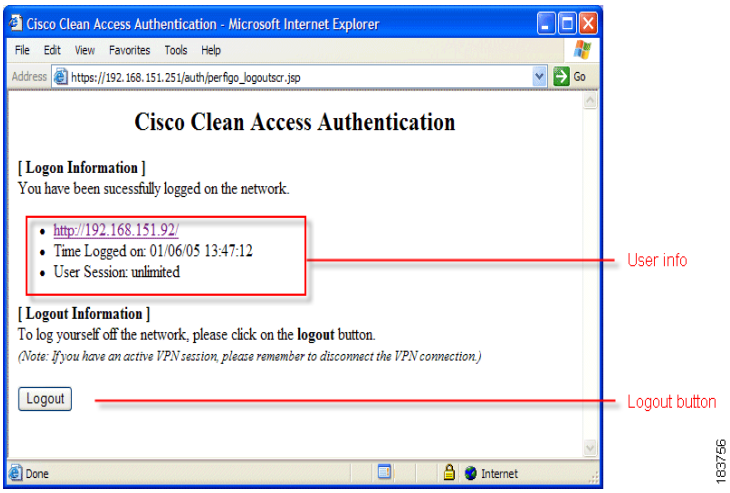
Note Typically, a new browser is opened when a redirect page is specified. If pop-up blockers are enabled on the client, Cisco NAC Appliance will use the main browser window as the Logout page in order to show login status, logout information and VPN information (if any).

Note High encryption (64-bit or 128-bit) is required for client browsers for web login and Agent authentication.

Specify Logout Page Information

After a successful login, the logout page pops up in its own browser on the client machine (Figure 5-11), usually behind the login success browser.

Figure 5-11 Logout Page


Cisco Clean Access Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.151.251/auth/perfigo_logoutscr.jsp
Go
Cisco Clean Access Authentication
[Logon Information]
You have been sucessfully logged on the network.
http://192.168.151.92/
Time Logged on: 01/06/05 13:47:12
User Session: unlimited
User info
[Logout Information]
To log yourself off the network, please click on the logout button.
(Note: If you have an active VPN session, please remember to disconnect the VPN connection.)
Logout
Logout button
Done
Internet
183756

You can specify the information that appears on the logout page by role as follows:

1. Go to the **User Management > User Roles > List of Roles** page.
2. Click the **Edit** icon next to the role for which you want to specify logout page settings.
3. In the **Edit Role** page (Figure 5-10), click the corresponding **Show Logged on Users** options to display them on the Logout page:
   - **User info** – Information about the user, such as the username.
   - **Logout** button – A button for logging off the network.

Note If no options are selected, the logout page will not appear.

See Create Local User Accounts, page 6-15 for further details.

Guest User Access

Guest access makes it easy to provide visitors or temporary users limited access to your network. The following are two methods to implement guest access:

Configure Guest User Registration—You can require guest users to register on the network by providing a set of credentials that identify that particular user on the CAM for the duration of the guest user session. Registered guest users share the network with authenticated users, but only get access to the network resources you specify in the guest user authentication role.

Enable the Preset "Guest" User Account—With the guest account method, guest users share the network with authenticated users. The Event Log displays all guest users with username "guest" but will differentiate each guest user by login timestamp and MAC/IP address (if L2) or IP address (if L3).

Note Guest users accessing the Cisco NAC Appliance system via the preset "Guest" user account must use the "Local DB" provider option. For more information, see Customize Login Page Content, page 5-8.

Configure Guest User Registration

Guest user registration allows guest users to log in using their own individual login ID independent of any existing local user accounts. Guest users enter any login credentials that identify that user's session(s) on the NAC Appliance system and those credentials identify that user on the CAM for the duration of the guest user session. Users can enter ID numbers, Email addresses, names, or any of a number of identifiers you specify when configuring guest user registration parameters on the CAM. This method allows guest users to submit unique user ID strings so that the administrator can track, manage, and display user sessions with meaningful identifiers. The identifier the user submits in the login page appears in the **Online Users** and **User Management > Guest Users** pages while the Guest user is logged in. (The alternate guest account method described below—Enable the Preset "Guest" User Account—does not record any specific individual information for any users and all users on the system appear as "guest.")

To enable Guest Registration on the NAC Appliance system:

1. Create a new Guest user role as you would any other user login role using the **User Management > User Roles > New Role** page as described in Create User Roles, page 6-2.
2. Configure the Guest authentication provider type and map it to the Guest role as described in Guest, page 7-26.
3. Configure the user login page to require Guest registration (as described in Customize Login Page Content, page 5-8) in the **Administration > User Pages > Login Page > List | Edit > Content** page:
   - Enable the **Provider Label** and click the checkbox corresponding to the Guest authentication provider type you have configured under **Available Providers** to ensure it appears in the list of available authentication sources in the **Providers** options users see on the login page.
   - Enable *both* the **Guest Label** and **Guest Registration Required** options to ensure users see the Guest login option on the login page.

Note If you do not enable all of these options on the **Administration > User Pages > Login Page**, Guest User Registration users do not see the option to log in as a guest.

- After you save your changes, click **View** to see how your customized page will appear to users. Figure 5-6 on page 5-11 illustrates how each field correlates to elements of the generated login page.

4. Configure the Guest User Access page as described in Configuring the Guest User Access Page, next. (This is an optional part of configuring Guest User registration. If you choose, you can accept the default NAC Appliance behavior for guest registration.)

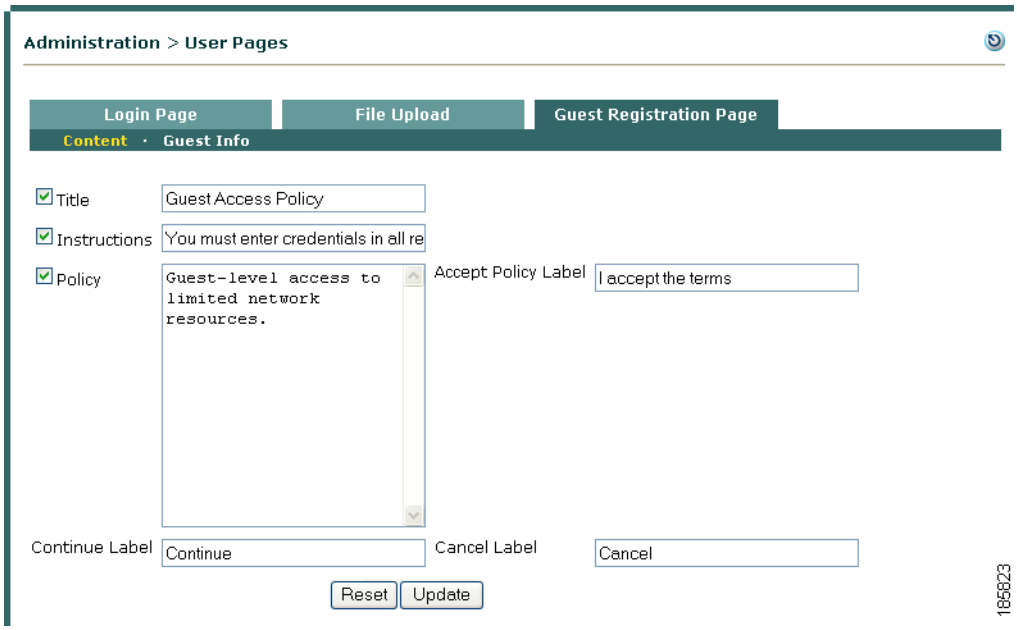
Configuring the Guest User Access Page

To configure a guest user access page:

Step 1 Be sure you have performed the preliminary steps under Configure Guest User Registration, page 5-17 before you configure the Guest registration options described in this procedure.

Step 2 Go to **Administration > User Pages > Guest Registration Page > Content**.

Figure 5-12 Administration > user Pages > Guest Registration Page > Content



Step 3 Specify parameters for the Guest Registration Page login settings or accept the default values:

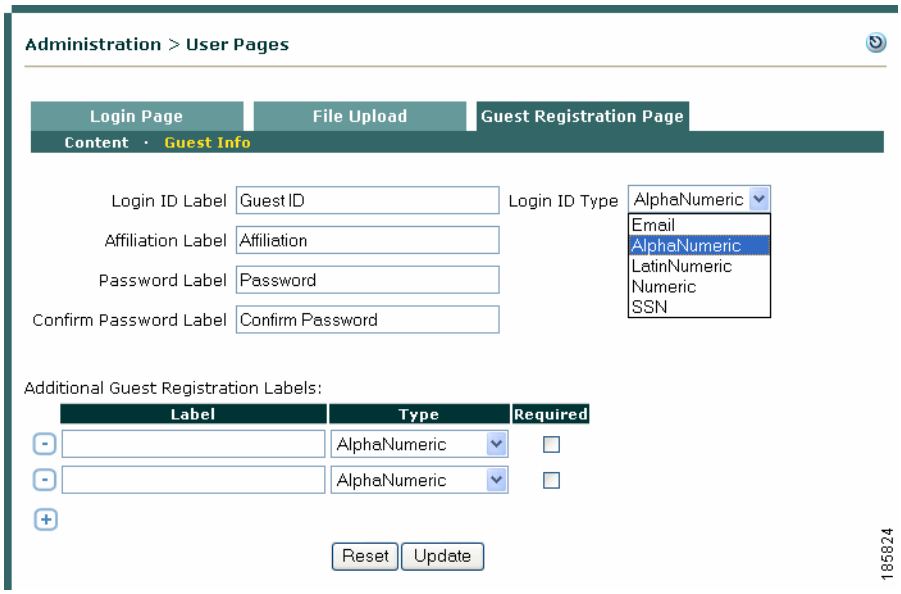
- **Title**—The heading guest users see at the top of the guest registration and credentials dialogs.
- **Instruction**—Any additional instructions, messages, cautions, or warnings you want to be sure guest users see before accessing the network. The text you specify appears under the credential-entry fields in the user credential dialog (see Figure 5-15).

- **Policy** and **Accept Policy Label**—(Optional) If you enable and specify text for the **Policy** and **Accept Policy Label** settings, the guest login dialog prompts the user to "accept" the guest access policy you enter (see Figure 5-14) by clicking the checkbox before clicking **Continue**. Otherwise, the guest user sees the credentials dialog (Figure 5-15) when they first attempt to log in to the NAC Appliance system.
- **Continue Label**—Allows you to specify text for the "log in" button users see in the guest access dialogs. (For example, you might choose to use "Log In," "Sign In," or "Connect.")
- **Cancel Label**—Allows you to specify text for the "cancel" button users see in the guest access dialogs.

Step 4 Click **Update** to change the appearance of the Guest Registration Page according to any settings you have updated or click **Reset** to return the page parameters/values to previously saved settings.

Step 5 Go to **Administration > User Pages > Guest Registration Page > Guest Info**.

Figure 5-13 Administration > user Pages > Guest Registration Page > Guest Info



Step 6 Specify parameters for the Guest Registration Page guest information settings (see Figure 5-15) or accept the default values:

- **Login ID Label** and **Login ID Type**—The text guest users see in the user ID entry field of the credentials dialog and the type of entry the NAC Appliance system is looking for from the guest user. The available options in the **Login ID Type** dropdown menu are:

Table 5-1 Login ID Type Settings

Login ID Type	Description	Example Guest User Entry
Email	A valid Email address (must include "@")	`guest_user@company.com`
AlphaNumeric	A text entry defining a name or other identifier comprised of just letters and numbers	`Jane Doe` `Contractor 12345`
LatinNumeric	A text entry defining a name or other identifier including special characters	`£100-500¥` `no @#($&!^] way`

Table 5-1 Login ID Type Settings

Login ID Type	Description	Example Guest User Entry
Numeric	A strictly digit-based string defining the user ID	543212345
SSN	The guest user's social security number	123-45-6789

- **Affiliation Label**—The text guest users see in the user affiliation entry field of the credentials dialog. (Other examples include "Company," "Vendor," "Contractor," or "Guest of.")
- **Password Label**—The text guest users see in the password entry field of the credentials dialog.
- **Confirm Password Label**—The text guest users see in the confirm password entry field of the credentials dialog.

Step 7 (Optional) Under Additional Guest Registration Labels, you can configure and specify settings for additional personalized text-entry fields guest users see when they go to enter login credentials:

a. Click the blue "plus" **+** symbol to create a new text-field entry.

b. Specify the Registration Label **Type** by selecting one of the options from the dropdown list. The available types and behavior include those defined in Table 5-1 and the following:

Table 5-2 Additional Registration Label Type Settings

Label ID Type	Description	Example guest user entry
US Phone Number	A standard North American regional 10-digit phone number (with or without delimiting hyphens)	555-555-5555 5555555555
Date	A text entry defining a name or other identifier comprised of just letters and numbers	11/11/2000 11-11-2000
ANY	Any text entry (including special characters)	£100-500¥ @#($&!^] UsEr-00-$@#*(MyID]

c. Specify a **Label** for the text field. (For example, if you specify that the additional entry should be a date, you might want to use the label "Today's Date.")

d. Specify whether or not the new additional text-entry field is **Required** by enabling or disabling the associated checkbox, as appropriate.

Step 8 Click **Update** to change the appearance of the Guest Registration Page according to any settings you have updated or click **Reset** to return the page parameters/values to previously saved settings.

After you enable Guest Registration and update the settings on the Guest Registration Content and Guest Info pages, guest users see login dialogs similar to Figure 5-14 and Figure 5-15 when they sign in to the NAC Appliance system.

Figure 5-14 Example Guest "Accept Policy" Dialog

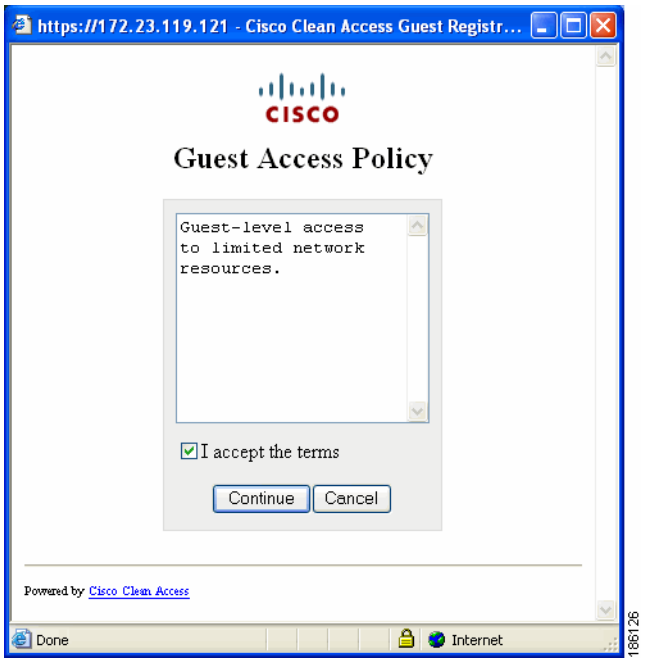


Figure 5-15 Example Guest Credentials Dialog



Enable the Preset "Guest" User Account

At installation, the Clean Access Manager includes a built-in guest user account. By default, the local user "guest" belongs to the Unauthenticated Role and is validated by the Clean Access Manager itself (Provider: LocalDB). You should specify a different role for the guest user and configure that role with login redirection, traffic control, and timeout policies as appropriate for guest users on your network.

With this method, the **Guest Access** button is enabled on the user login page. When a visitor clicks the button, the username and password **`guest`**/**`guest`** are sent to the CAM for authentication, and the guest user can be immediately redirected to the desired web page. Note that you must configure a new user role to which to associate the guest user.

1. Create a new Guest user role as you would any other user login role using the **User Management > User Roles > New Role** page as described in Create User Roles, page 6-2.
2. Associate the Guest user to a Guest role as described in Create or Edit a Local User, page 6-15.
3. Configure Traffic Policies for the Guest role as described in Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule".
4. Configure the user login page to enable Guest access as described in Configuring the Guest User Access Page, page 5-18.

Note Cisco recommends using the guest login method described in Configure Guest User Registration, page 5-17 over both this "Enable Login Page Guest Access" option and the **Allow All** method. (Earlier releases of Cisco NAC Appliance also allowed guest users to log in by submitting their email address and gain network access via the **Allow All** provider type. The user ID the guest user submitted in the login page (e.g., their email address) would appear as the **User Name** in the **Online Users** page while the user was logged in.)



User Management: Configuring User Roles and Local Users

This chapter describes the following topics:

- Overview, page 6-1
- Create User Roles, page 6-2
- Create Local User Accounts, page 6-15

For details on configuring authentication servers, see Chapter 7, "User Management: Configuring Authentication Servers."

For details on creating and configuring the web user login page and guest users, see Chapter 5, "Configuring User Login Page and Guest Access."

For details on configuring traffic policies for user roles, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

Overview

This chapter describes the user role concept in Cisco NAC Appliance. It describes how user roles are assigned and how to create and configure them. It also describes how to create local users that are authenticated internally by the CAM (used primarily for testing).

Cisco NAC Appliance network protection features are configured for users by role and operating system. The following roles are employed when users are in the Cisco NAC Appliance network (i.e. during the time they are In-Band) and must be configured with traffic policies and session timeout:

- **Unauthenticated Role**—Default system role for unauthenticated users (Agent or web login) behind a Clean Access Server. Web login users are in the unauthenticated role while network scanning is performed.
- **Normal Login Role**—There can be multiple normal login roles in the system. A user is put into a normal login role after a successful login.
- **Client Posture Assessment Roles** (Agent Temporary Role and Quarantine Role)—Agent users are in the Temporary role while Agent Requirements are checked on their systems. Both web login and Agent users are put in the Quarantine role when network scanning determines that the client machine has vulnerabilities.

Note that the Temporary and Quarantine roles are intended to have limited session time and network access in order for users to fix their systems.

When a user authenticates, either through the web login page or Agent, Cisco NAC Appliance determines the normal login role of the user and the requirements and/or network scans to be performed for the role. Cisco NAC Appliance then performs requirement checking and/or network scanning as configured for the role and operating system.

Note that while the role of the user is determined immediately after the initial login (in order to determine the scans or system requirements associated with the user), a user is not actually put into a normal login role until requirements are met, scanning has occurred and no vulnerabilities are found. If the client has not met requirements, the user stays in the Agent Temporary role until requirements are met or the session times out, including when the user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example) and the **Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs** option in the CAM **Device Management > Clean Access > General Setup > Agent Login** web console page has not been enabled. If the user has met requirements but is found with network scanning vulnerabilities, the user can be assigned to a quarantine role or simply blocked, depending on the configuration.

Create User Roles

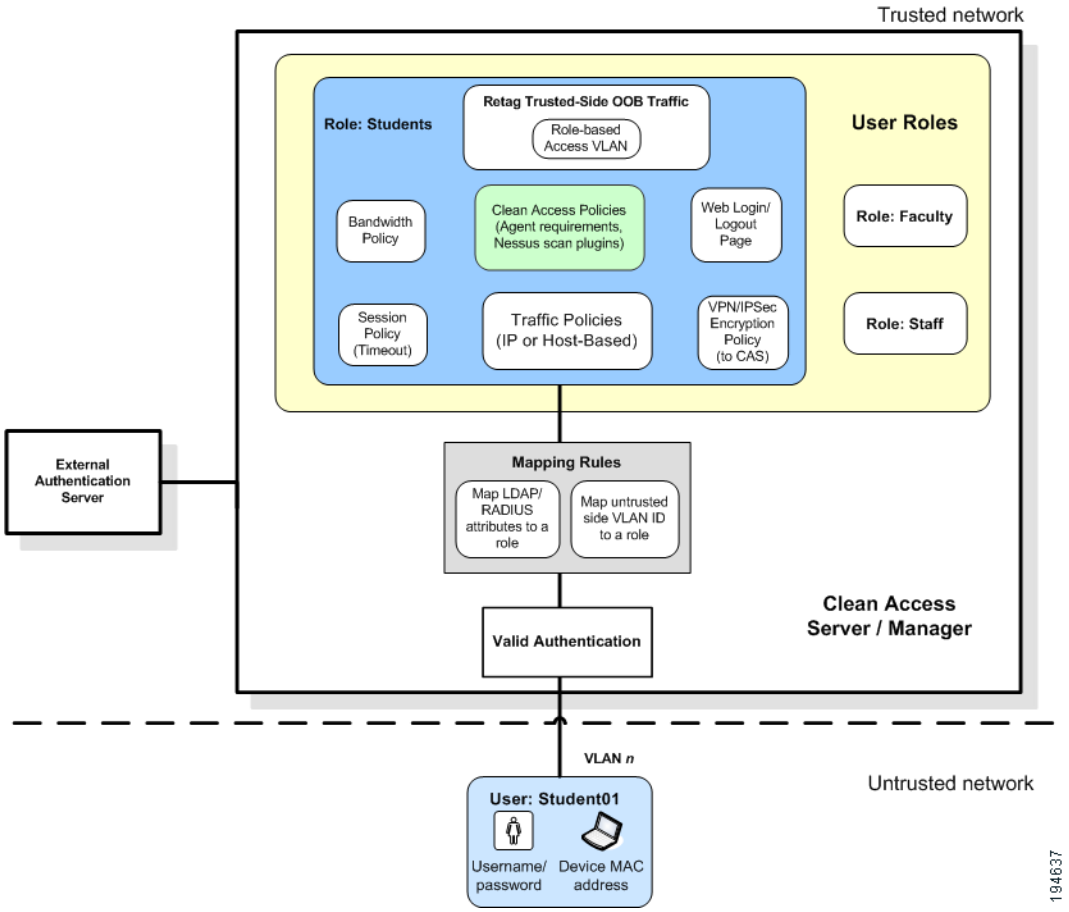
Roles are integral to the functioning of Cisco NAC Appliance and can be thought of in the following ways:

- As a classification scheme for users that persists for the duration of a user session.
- As a mechanism that determines traffic policies, bandwidth restrictions, session duration, posture assessment, and other policies within Cisco NAC Appliance for particular groups of users.

In general, roles should be set up to reflect the shared needs of distinct groups of users in your network. Before creating roles, you should consider how you want to allocate privileges in your network, apply traffic control policies, or group types of client devices. Roles can frequently be based on existing groups within your organization (for example, students/faculty/staff, or engineering/sales/HR). Roles can also be assigned to groups of client machines (for example, gaming boxes). As shown in Figure 6-1, roles aggregate a variety of user policies including:

- Traffic policies
- Bandwidth policies
- VLAN ID retagging
- Cisco NAC Appliance network port scanning plugins
- Agent client machine requirements

Figure 6-1 Normal Login User Roles



User Role Types

The system puts a user in a role when the user attempts to log in. There are four default user role types in the system: Unauthenticated Role, Normal Login role, Agent Temporary role, and Quarantine role.

Unauthenticated Role

There is only one Unauthenticated Role and it is the system default role. If a configured normal login role is deleted, users in that role are reassigned to the Unauthenticated Role (see Delete Role, page 6-15). You can configure traffic and other policies for the Unauthenticated Role, but the role itself cannot be edited or removed from the system.

Users on the untrusted (managed) side of the Clean Access Server are in the Unauthenticated role prior to the initial web login or Agent login. When using web login/network scanning only, users remain in the Unauthenticated role until clients pass scanning (and are transferred to a normal login role), or fail scanning (and are either blocked or transferred to the quarantine role).

Normal Login Role

There can be multiple normal login roles (including "restricted access" roles) in the system. A user is put into a normal login role after a successful login. You can configure normal login roles to associate users with the following:

- Network access traffic control policies—what parts of the network and which application ports can users can access while in the role.
- VLAN ID:
  - For In-Band users, retag traffic (to/from users in the role) destined to the trusted network to differentiate priority to the upstream router.
  - For Out-of-Band (OOB) users, set the Access VLAN ID for users in the role if using role-based configuration.
- Cisco NAC Appliance network scanning plugins—the Nessus port scanning to perform, if any.
- Agent requirements—the software package requirements client systems must have.
- End-user HTML page(s) displayed after successful or unsuccessful web logins —the pages and information to show to web login users in various subnets/VLANs/roles. See Chapter 5, "Configuring User Login Page and Guest Access" for further details.

Typically, there are a number of normal login roles in a deployment, for example roles for Students, Faculty, and Staff (or Engineering, HR, Sales). You can assign normal login roles to users in several ways:

- By the MAC address or subnet of a client device.
  You can assign a role to a device or subnet through **Device Management > Filters**. See Global Device and Subnet Filtering, page 2-10 for details.
- By local user attributes. Local users are primarily used for testing and are authenticated internally by the Clean Access Manager rather than an external authentication server. You can assign a role to a local user through **User Roles > Local Users**. See Create Local User Accounts, page 6-15.
- By external authentication server attributes. For users validated by an external authentication server, the role assigned can be based on:
  - The untrusted network VLAN ID of the user.
    This allows you to use untrusted network information to map users into a user role.
  - The authentication attributes passed from LDAP and RADIUS authentication servers.
    This allows you to use authentication attributes to map different users to different roles within Cisco NAC Appliance. If no mapping rules are specified, users are assigned the default role specified for the authentication server, after login. VLAN mapping and attribute mapping is done through **User Management > Auth Servers > Mapping Rules**.

  For details, see Adding an Authentication Provider, page 7-4 and Map Users to Roles Using Attributes or VLAN IDs, page 7-31.

Role Assignment Priority

Note that the order of priority for role assignment is as follows:

1. MAC address
2. Subnet / IP Address
3. Login information (login ID, user attributes from auth server, VLAN ID of user machine, etc.)

Therefore, if a MAC address associates the client with “Role A”, but the user’s login ID associates him or her to “Role B”, “Role A” is used.

For additional details, see also Global Device and Subnet Filtering, page 2-10 and Device Filters for Out-of-Band Deployment, page 2-14.

Client Posture Assessment Roles

You can implement client posture assessment in Cisco NAC Appliance as network scanning only (see Figure 12-1 on page 12-2), Agent only, or Agent with network scanning. With posture assessment configured, two types of roles are used specifically for Cisco NAC Appliance:

- **Agent Temporary Role**

  When the Agent is used, the Agent Temporary role is assigned to users after authentication to allow the user limited network access to download and install required packages that will prevent the user’s system from becoming vulnerable. The user is prevented from normal login role access to the network until the Agent requirements are met.

  There is only one Agent Temporary role in the system. This role is only in effect when the user is required to use Agent to login and pass Agent requirements.

  The Agent Temporary role is assigned to users for the following time periods:

  a. From the login attempt until successful network access. The client system meets Agent requirements and is not found with vulnerabilities after network scanning. The user transfers from the Agent Temporary role into the user’s normal login role.

  b. From the login attempt until Agent requirements are met. The user has the amount of time configured in the Session Timer for the role to download and install required packages. If the user cancels or times out, the user is removed from the Agent Temporary role and must restart the login process. If the user downloads Agent requirements within the time allotted, the user stays in the Agent Temporary role and proceeds to network scanning (if enabled).

  Note If the user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example), and the **Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs** option in the CAM **Device Management > Clean Access > General Setup > Agent Login** web console page has not been enabled, the client machine remains in the Temporary role until the Session Timer expires and the user is given the opportunity to perform login/remediation again.

  c. From the login attempt until network scanning finds vulnerabilities on the user system. If the client system meets Agent requirements, but is found to have vulnerabilities during network scanning, the user is transferred from the Agent Temporary role into the quarantine role.

- **Quarantine Role**

  With network scanning enabled, the purpose of the Agent quarantine role is to allow the user limited network access to resources needed to fix vulnerabilities that already exist on the user system. The user is prevented from normal login role access to the network until the vulnerabilities are fixed.

  There can be one or multiple quarantine roles in the system. A user is put into a quarantine role if:

  – The user attempts to log in using the web login page, and network scanning finds a vulnerability on the user system.

– The user logs in using the Agent and meets requirements but network scanning finds a vulnerability on the user system.

The user has the amount of time configured in the Session Timer for the role to access resources to fix vulnerabilities. If the user cancels or times out, the user is logged out of the quarantine role and must restart the login process. At the next login attempt, the client again goes through posture assessment.

When the user fixes vulnerabilities within the time allotted, if the Agent is used to log in, the user can go through network scanning again during the same session. If web login is used, the user must log out or time out then login again for the second network scanning to occur.

Note When using web login, the user should be careful not to close the Logout page (see Figure 5-11 on page 5-16). If the user cannot not log out but reattempts to login before the session times out, the user is still considered to be in the original quarantine role and is not redirected to the login page.

Only when the user has met requirements and fixed vulnerabilities is the user allowed network access in the corresponding normal login role. You can map all normal login roles to a single quarantine role, or you can create and customize different quarantine roles. For example, multiple quarantine roles can be used if different resources are required to fix vulnerabilities for particular operating systems. In either case, a normal login role can only be mapped to one quarantine role. After the roles are created, the association between the normal role and quarantine role is set up in the **Device Management > Clean Access > General Setup** form. See Client Login Overview, page 1-6 for details.

Session Timeouts

You can also limit network access with brief session timeouts and restricted traffic policy privileges. The session timeout period is intended to allow users only a minimum amount of time to complete posture assessment and remediation. A minimal timeout period for client posture assessment-related roles:

- Limits the exposure of vulnerable users to the network.
- Prevents users from full network access in the Temporary role. This is to limit users from circumventing rechecks if they fail a particular check, install the required package, restart their computers, but do not manually log out.

Factors in determining the timeout period appropriate for your environment include the network connection speed available to users and the download size of packages you will require.

You can additionally configure a Heartbeat Timer to log off all users if the CAS cannot connect to the clients after a configurable number of minutes. See Configure User Session and Heartbeat Timeouts, page 8-15 for further details.

You can configure **Max Sessions per User Account** for a user role. This allows administrators to limit the number of concurrent machines that can use the same user credentials. The feature allows you to restrict the number of login sessions per user to a configured number. If the online login sessions for a username exceed the value specified (1–255; 0 for unlimited), the web login page or the Agent will prompt the user to end all sessions or end the oldest session at the next login attempt. See Role Properties, page 6-9 for details.

Default Login Page

A default login page must be added and present in the system in order for both the web login and Agent users to authenticate.

The login page is generated by Cisco NAC Appliance and is shown to end users by role. When users first try to access the network from a web browser, an HTML login page appears prompting the users for a user name and password. Cisco NAC Appliance submits these credentials to the selected authentication provider and uses them determine the role in which to put the user. You can customize this web login page to target the page to particular users based on a user's VLAN ID, subnet, and operating system.

Caution If a default login page is not present, Agent users will see an error dialog when attempting login ("Clean Access Server is not properly configured, please report to your administrator.").

Note For L3 OOB deployments, you must also Enable Web Client for Login Page, page 5-5.

For details on creating and configuring the web user login page, see Chapter 5, "Configuring User Login Page and Guest Access." To quickly add a default login page, see Add Default Login Page, page 5-3.

Traffic Policies for Roles

When you first create a role, it has a default traffic filtering policy of "deny all" for traffic moving from the untrusted side to the trusted side, and "allow all" for traffic from the trusted side to the untrusted side. Therefore, after creating the role, you need to create policies to permit the appropriate traffic. See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" for details on how to configure IP-based and host-based traffic policies for user roles.

In addition, traffic policies need to be configured for the Agent Temporary role and the quarantine role to prevent general access to the network but allow access to web resources or remediation sites necessary for the user to meet requirements or fix vulnerabilities.See Configure Policies for Agent Temporary and Quarantine Roles, page 8-19 for details.

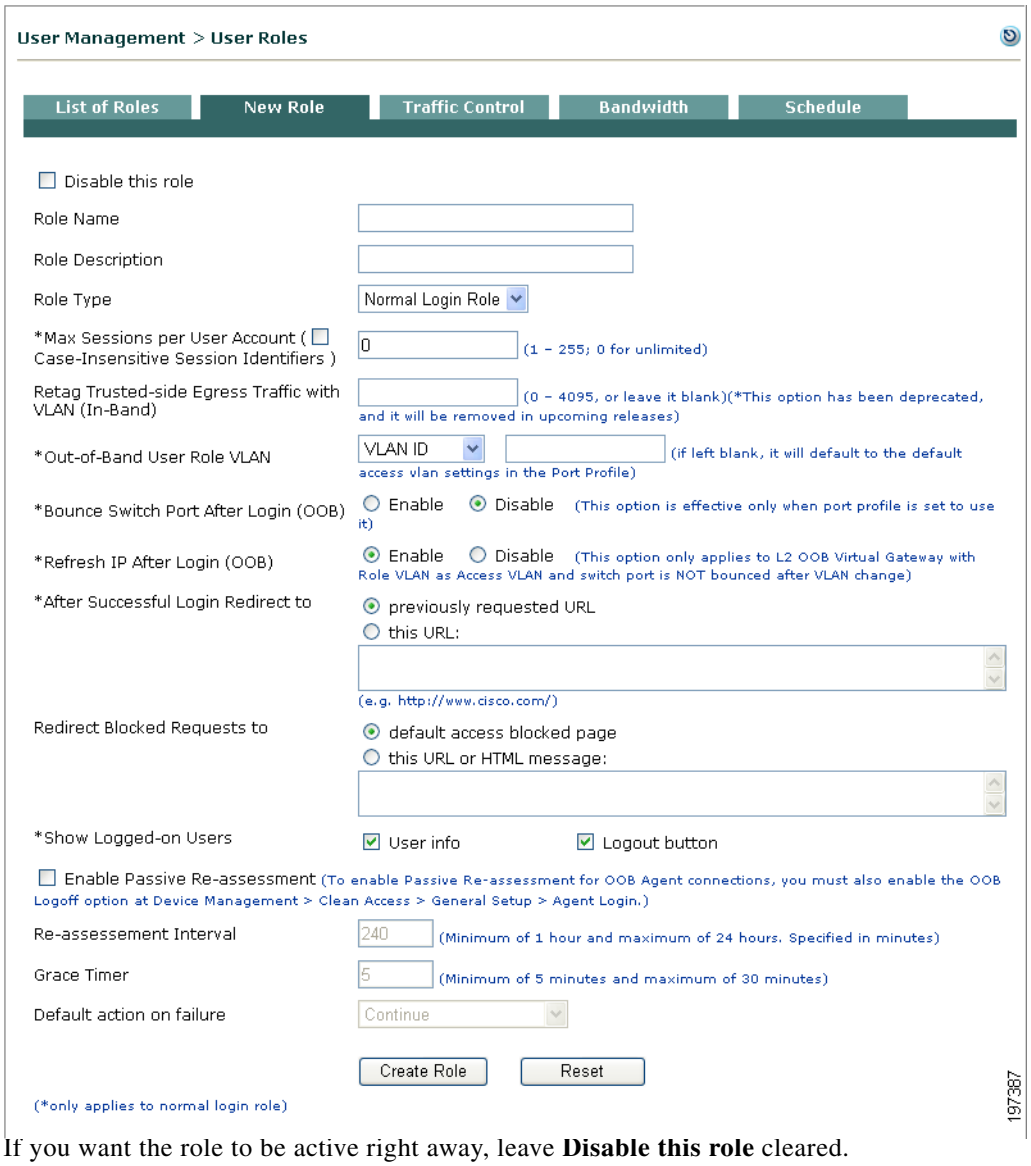
Adding a New User Role

The Agent Temporary role and a Quarantine role already exist in the Cisco NAC Appliance system and only need to be configured to meet your specific network needs. However, normal login roles (or any additional quarantine roles) must first be added. Once a new role is created, it can then be associated to the traffic policies and other properties you customize in the web console for your environment.

Note For new roles, traffic policies must be added to allow traffic from the untrusted to the trusted network. See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" for details.

Step 1 Go to **User Management > User Roles > New Role** (Figure 6-2).

Figure 6-2 Add New User Role


User Management > User Roles
List of Roles
New Role
Traffic Control
Bandwidth
Schedule
Disable this role
Role Name
Role Description
Role Type
Normal Login Role
*Max Sessions per User Account (Case-Insensitive Session Identifiers)
0
(1 – 255; 0 for unlimited)
Retag Trusted-side Egress Traffic with VLAN (In-Band)
(0 – 4095, or leave it blank)(*This option has been deprecated, and it will be removed in upcoming releases)
*Out-of-Band User Role VLAN
VLAN ID
(if left blank, it will default to the default access vlan settings in the Port Profile)
*Bounce Switch Port After Login (OOB)
Enable
Disable
(This option is effective only when port profile is set to use it)
*Refresh IP After Login (OOB)
Enable
Disable
(This option only applies to L2 OOB Virtual Gateway with Role VLAN as Access VLAN and switch port is NOT bounced after VLAN change)
*After Successful Login Redirect to
previously requested URL
this URL:
(e.g. http://www.cisco.com/)
Redirect Blocked Requests to
default access blocked page
this URL or HTML message:
*Show Logged-on Users
User info
Logout button
Enable Passive Re-assessment (To enable Passive Re-assessment for OOB Agent connections, you must also enable the OOB Logoff option at Device Management > Clean Access > General Setup > Agent Login.)
Re-assessement Interval
240
(Minimum of 1 hour and maximum of 24 hours. Specified in minutes)
Grace Timer
5
(Minimum of 5 minutes and maximum of 30 minutes)
Default action on failure
Continue
Create Role
Reset
(*only applies to normal login role)
197387

Step 2 If you want the role to be active right away, leave **Disable this role** cleared.

Step 3 Type a unique name for the role in the **Role Name** field.

Step 4 Type an optional **Role Description**.

Step 5 For the **Role Type**, choose either:

- **Normal Login Role** – Assigned to users after a successful login. When configuring mapping rules for authentication servers, the attributes passed from the auth server are used to map users into normal login roles. Network scan plugins and Agent requirements are also associated to a normal login role. When users log in, they are scanned for plugins and/or requirements met (while in the unauthenticated/Temporary role). If users meet requirements and have no vulnerabilities, they gain access to the network in the normal login role.

Note Form fields that only apply to normal login roles are marked with an asterisk (*).

- **Quarantine Role** – Assigned to users to quarantine them when network scanning finds a vulnerability on the user system. Note that a system Quarantine role already exists and can be configured. However, the New Role form allows you to add additional quarantine roles if needed.

Step 6 See Role Properties, page 6-9 for configuration details on each role setting.

Note If planning to use role-based profiles with an OOB deployment, you must specify the Access VLAN in the **Out-of-Band User Role VLAN** field when you create the user role. For further details see Out-of-Band User Role VLAN, page 6-10 and Add Port Profile, page 3-34.

Step 7 When finished, click **Create Role**. To restore default properties on the form click **Reset**.

Step 8 The role now appears in the **List of Roles** tab.

Step 9 If creating a role for testing purposes, the next step is to create a local user to associate to the role. See Create Local User Accounts, page 6-15 next.

Role Properties

Table 6-1 details all the settings in the **New/Edit Role** (Figure 6-2) form.

Table 6-1 Role Properties

Control	Description
Disable this role	Stops the role from being assigned to new users.
Role Name	A unique name for the role.
Role Description	An optional description for the role.
Role Type	Whether the role is a **Normal Login Role** or a client posture assessment-related role: **Quarantine Role** or **Agent Temporary Role**. See User Role Types, page 6-3 for details.
Max Sessions per User Account (Case-Insensitive)	The **Max Sessions per User Account** option allows administrators to limit the number of concurrent machines that can use the same user credentials. The feature allows you to restrict the number of login sessions per user to a configured number. If the online login sessions for a username exceed the value specified (1 – 255; 0 for unlimited), the web login page or the Agent will prompt the user to end all sessions or end the oldest session at the next login attempt. The **Case-Insensitive** checkbox allows the administrator to allow/disallow case-sensitive user names towards the max session count. For example, if the administrator chooses to allow case-sensitivity (box unchecked; default), then `jdoe`, `Jdoe`, and `jDoe` are all treated as different users. If the administrator chooses to disable case-sensitivity (box checked), then `jdoe`, `Jdoe`, and `jDoe` are treated as the same user.
Retag Trusted-side Egress Traffic with VLAN (In-Band)	**Note** **This feature is deprecated and will be removed in future releases**.

Table 6-1 Role Properties (continued)

Control	Description
Out-of-Band User Role VLAN	**Out-of-Band (OOB) Configuration —Retag Trusted-side Traffic with Role VLAN** Once a user has finished posture assessment and remediation, if needed, and the client device is deemed to be "certified," the switch port to which the client is connected can be assigned to a different Access VLAN based on the value specified in the **Out-of-Band User Role VLAN** field. Hence, users connecting to the same port (at different times) can be assigned to different Access VLANs based on this setting in their user role. For OOB deployment, if configuring role-based VLAN switching for a controlled port, you must specify an Access VLAN ID when you create the user role. When an Out-of-Band user logs in from a managed switch port, the CAM will: • Determine the role of the user based on the user's login credentials. • Check if role-based VLAN switching is specified for the port in the Port Profile. • Switch the user to the Access VLAN, once the client is certified, according to the value specified in the **Out-of-Band User Role VLAN** field for the user's role. Admins can specify **VLAN Name** or **VLAN ID** on the **New/Edit User Role** form. **VLAN Name** is case-sensitive. If specifying wildcards for VLAN Name, you can use: abc, *abc, abc*, *abc*. The switch will use the first match for wildcard VLAN Name. You can only specify numbers for **VLAN ID** If the switch cannot find the VLAN specified (e.g. VLAN Name is mistyped), the error will appear on the perfigo.log (not the Event Log). For additional details, see Global Device and Subnet Filtering, page 2-10 and Chapter 3, "Switch Management: Configuring Out-of-Band Deployment."
Bounce Switch Port After Login (OOB)	If you have first enabled the **Bounce the port based on role settings after VLAN is changed** option on the **OOB Management > Profiles > Port > New/Edit** page, the Agent does *not* renew the IP address on the client machine after login and posture assessment. **Note** This option only applies when a port profile is configured to use it.
Refresh IP After Login (OOB)	When enabled, the switch port through which the user is accessing the network is not bounced when the VLAN changes from the Authentication VLAN to the Access VLAN. Instead, the Agent renews/refreshes the IP address on the client machine following login and posture assessment. This option only applies when the Port profile is configured to **Bounce the port based on role settings after VLAN is changed** under **OOB Management > Profiles > Port > New/Edit** (see Add Port Profile, page 3-34). See DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6 for additional information on configuring client IP refresh/renew. **Note** For information on Access to Authentication VLAN change detection for an OOB client machine, see Configure Access to Authentication VLAN Change Detection, page 3-67.

Table 6-1 Role Properties (continued)

Control	Description
After Successful Login Redirect to	When successfully logged in, the user is forwarded to the web page indicated by this field. You can have the user forwarded to: • **previously requested URL** – (default) The URL requested by the user before being redirected to the login page. • **this URL**– To redirect the user to another page, type "**http://**" and the desired URL in the text field. Note that **"http://**" must be included in the URL. **Note** Typically, a new browser is opened when a redirect page is specified. If pop-up blockers are enabled, Cisco NAC Appliance will use the main browser window as the Logout page in order to show login status, logout information and VPN information (if any). See also Redirect the Login Success Page, page 5-15.
Redirect Blocked Requests to	If the user is blocked from accessing a resource by a "**Block**" IP traffic policy for the role, users are redirected when they request the blocked page. You can have the user forwarded to: • **default access blocked page**—The default page for blocked access. • **this URL or HTML message**—A particular URL or HTML message you specify in the text field. See also Adding Traffic Policies for Default Roles, page 8-27.

Table 6-1 Role Properties (continued)

Control	Description
Show Logged-on Users	The information that should be displayed to web users in the Logout page. After the web user successfully logs in, the Logout page pops up in its own browser and displays user status based on the combination of options you select: • **User info**—Information about the user, such as the user name. • **Logout** button—A button for logging the user off the network (web Logout page only). See Specify Logout Page Information, page 5-16 for an example of a Logout page. **Note** For Agent users, a link to a VPN Info dialog is provided in the success login and taskbar menu if an Optional or Enforce VPN Policy is enabled for both the CAS and user role.

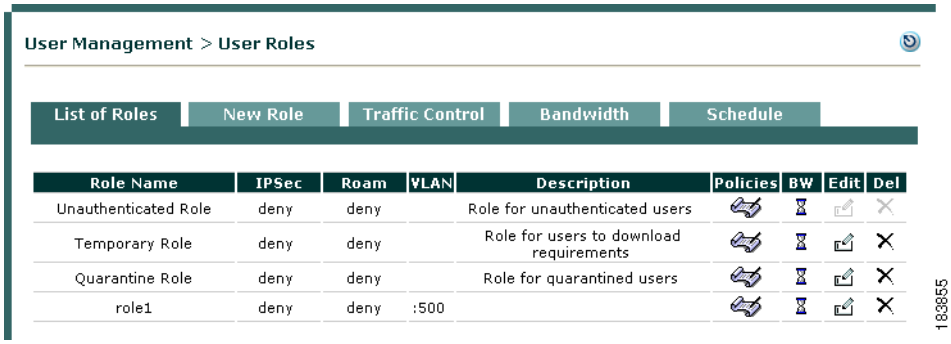
Table 6-1 Role Properties (continued)

Control	Description
Enable Passive Re-assessment	This option allows periodic re-assessment on client systems that are online to ensure continuous compliancy of the current network policies. This option is disabled by default. Passive Re-assessment enables the persistent Agent (Cisco NAC Agent) on the client machine to periodically verify that the client machine is still compliant with imposed network security policies without requiring the user to log out of Cisco NAC Appliance and go through posture assessment to "regain" network access. **Note** For OOB deployment, you *must* enable the Out-of-Band Logoff function in order to enforce Passive Re-assessment. See Configure Out-of-Band Logoff, page 9-6 for details. **Note** Passive Re-assessment is available for NAC Agent 4.8.0.32 or later only. **Note** While using Passive Re-assessment, the client should communicate with the same CAS that authenticated the user. • **Re-assessment Interval**—The time interval in minutes between the completion of login process and the first re-assessment, and between consecutive re-assessment attempts on the client machine. The timer starts once the login is completed successfully. The time can vary from 60 minutes (1 hour) to 1440 minutes (24 hours). The default value is 240 minutes (4 hours). • **Grace Timer**—The time in minutes for which the Agent waits for the users to remediate any failed posture checks, when the **Default action on failure** option has been set to **Allow user to remediate**. The time can vary from 5 minutes to 30 minutes. The default value is 5 minutes. • **Default action on failure**—Select the default action to be performed if the re-assessment fails: – **Continue**—The user can continue using the network. No interaction is required by the user with the agent. This is the selected by default. – **Allow user to remediate**—The user is prompted for remediation when there is a failure in any of the optional or mandatory requirements. If the user cancels the remediation, then the CAM receives a failed requirement report from the client machine performing Passive Re-Assessment. – **Logoff user immediately**—The user is logged out immediately when any of the mandatory requirements fails, and placed back to the unauthenticated network. The CAM/CAS keep track of the Passive Re-assessment reports and save failed reports, which can be viewed using the Clean Access Agent Report Viewer. If the servers do not receive any report from the Agent within a time interval, then the user is removed from the on-line user list. The maximum time interval for which the server waits is **Re-assessment Interval + 2 x Grace Timer**.

Modifying an Existing Temporary, Quarantine, or Login Role

From the **List of Roles** tab (Figure 6-3), you can configure traffic and bandwidth policies for any user role. You can also edit the Agent Temporary role, Quarantine role, and any normal login role you have created.

Figure 6-3 List of Roles



Operations you can perform from the **List of Roles** tab are as follows:

- The **Policies** icon links to the **Traffic Control** tab and lets you set traffic filter policies for the role. For details, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."
- The **BW** icon links to the **Bandwidth** tab and lets you set upstream and downstream bandwidth restrictions by role. For details, see Control Bandwidth Usage, page 8-13.
- The **Edit** icon links to the **Edit Role** tab and lets you modify role properties. See Editing an Existing Role, page 6-14 below.
- The **Delete** icon removes the role and all associated polices from the system and assigns users to the Unauthenticated role. See Delete Role, page 6-15.
- Specify a network access schedule for the role. For details, see Configure User Session and Heartbeat Timeouts, page 8-15.

Editing an Existing Role

Step 1 Go to **User Management > User Roles > List of Roles**.

Step 2 Roles listed will include the following:

- **Temporary Role**—Assigned to users to force them to meet Agent packages or requirements when Agent is required to be used for login and posture assessment. There is only one Agent Temporary Role which is already present in the system. This role can be edited but not added.
- **Quarantine Role**—Assigned to users to quarantine them when network scanning finds a vulnerability on the user system. You can configure the system Quarantine role only or add additional quarantine roles if needed.
- **User-defined role**—The user roles you have created.

Note You can configure traffic and bandwidth policies for the **Unauthenticated Role**, but otherwise this system default role cannot be edited or removed.

Step 3 Click the **Edit** icon next to a role to bring up the **Edit Role** form. An Edit Role window similar to that in Figure 6-2 appears.

Step 4 Modify role settings as desired. See Role Properties, page 6-9 for details.

Step 5 Click **Save Role**.

Delete Role

To delete a role, click the **Delete** icon next to the role in the **List of Roles** tab of the **User Management > User Roles** page. This removes the role and associated polices from the system and assigns users to the Unauthenticated role.

Users actively connected to the network in the deleted role will be unable to use the network. However, their connection will remain active. Such users should be logged off the network manually, by clicking the **Kick User** button next to the user in the **Monitoring > Online Users > View Online Users** page. The users are indicated in the online user page by a value of **Invalid** in the **Role** column.

Create Local User Accounts

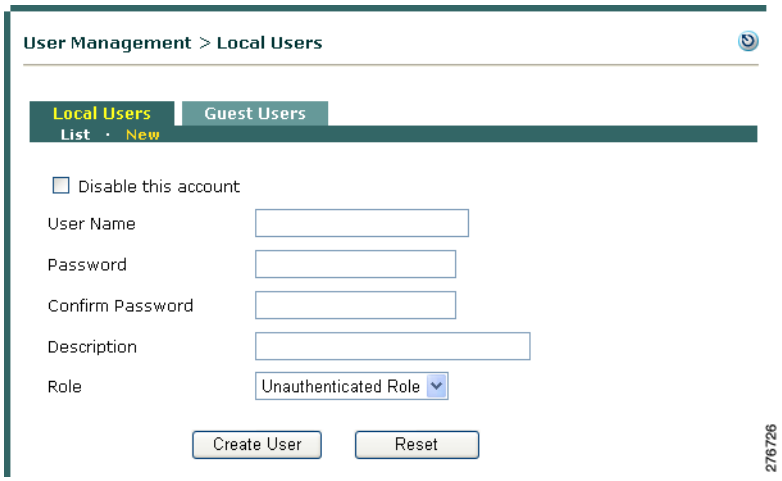
A local user is one who is validated by the Clean Access Manager itself, not by an external authentication server. Local user accounts are not intended for general use (the users cannot change their password outside of the administrator web console). Local user accounts are primarily intended for testing or for guest user accounts. For testing purposes, a user should be created immediately after creating a user role.

Create or Edit a Local User

Step 1 Go to **User Management > Local Users > Local Users** and:

- Choose the **New** subtab option.
- Choose the **List** subtab option and click the **Edit** icon for the user you want to update.

Figure 6-4 New Local User



Step 2 If you want the user account to be active immediately, be sure to leave the **Disable this account** check box cleared.

Step 3 Type a unique **User Name** for the user. This is the login name by which the user is identified in the system.

Step 4 Type a password in the **Password** field and retype it in the **Confirm Password** field. The password value is case-sensitive.

Step 5 Optionally, type a **Description** for the user.

Step 6 Choose the default role for the user from the **Role** list. All configured roles appear in the list. If the role you want to assign the user does not exist yet, create the role in the **User Roles** page and modify the user profile with the new role.

Step 7 When finished, click **Create User**.

The user now appears in the **List of Local Users** tab. From there, you can view user information, edit user settings such as the name, password, role, or remove the user.



User Management: Configuring Authentication Servers

This chapter describes how to set up external authentication sources, configure Active Directory Single Sign-On (SSO), VLAN ID or attribute-based auth server mapping rules, and RADIUS accounting. Topics are as follows:

- Overview, page 7-1
- Adding an Authentication Provider, page 7-4
- Configuring Authentication Cache Timeout (Optional), page 7-28
- Authenticating Against a Backend Active Directory, page 7-28
- Map Users to Roles Using Attributes or VLAN IDs, page 7-31
- Auth Test, page 7-39
- RADIUS Accounting, page 7-41

For details on AD SSO, see the "Configuring Active Directory Single Sign-On (AD SSO)" chapter in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

For details on creating and configuring the web user login page, see Chapter 5, "Configuring User Login Page and Guest Access."

For details on configuring user roles and local users, see Chapter 6, "User Management: Configuring User Roles and Local Users."

For details on configuring traffic policies for user roles, see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

Overview

By connecting the Clean Access Manager to external authentication sources, you can use existing user data to authenticate users and administrator users in the untrusted network. Cisco NAC Appliance supports several authentication provider types for the following two cases:

- When you want to work with an existing backend authentication server(s)
- When you want to enable any of the transparent authentication mechanisms provided by Cisco NAC Appliance

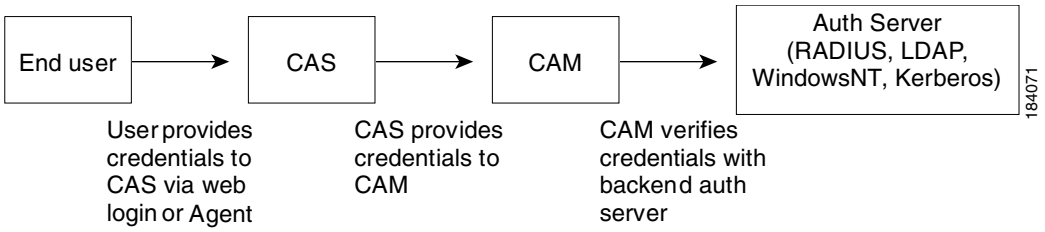
Working with Existing Backend Authentication Servers

When working with existing backend authentication servers, Cisco supports the following authentication protocol types:

- Kerberos
- RADIUS (Remote Authentication Dial-In User Service)
- Windows NT (NTLM Auth Server)
- LDAP (Lightweight Directory Access Protocol)

When using this option, the CAM is the authentication client which communicates with the backend auth server. Figure 7-1 illustrates the authentication flow.

Figure 7-1 Cisco NAC Appliance Authentication Flow with Backend Auth Server


End user
CAS
CAM
Auth Server (RADIUS, LDAP, WindowsNT, Kerberos)
184071
User provides credentials to CAS via web login or Agent
CAS provides credentials to CAM
CAM verifies credentials with backend auth server

Currently, it is required to use RADIUS, LDAP, Windows NT, or Kerberos auth server types if you want to enable Cisco NAC Appliance system features such as:

- Network scanning policies
- Agent requirements
- Attribute-based auth mapping rules

Note For Windows NT only, the CAM must be on the same subnet as the domain controllers.

Working with Transparent Auth Mechanisms

When using this option, Cisco supports the following authentication protocol types:

- Active Directory SSO
- Cisco VPN SSO
- Windows NetBIOS SSO (formerly known as “Transparent Windows”)
- S/Ident (Secure/Identification)

Depending on the protocol chosen, the Clean Access Server sniffs traffic relevant to the authentication source flowing from the end user machine to the auth server (for example, Windows logon traffic for the Windows NetBIOS SSO auth type). The CAS then uses or attempts to use that information to authenticate the user. In this case, the user does not explicitly log into the Cisco NAC Appliance system (via web login or Agent).

Note S/Ident and Windows NetBIOS SSO can be used for authentication only—posture assessment, quarantining, and remediation do not currently apply to these auth types.

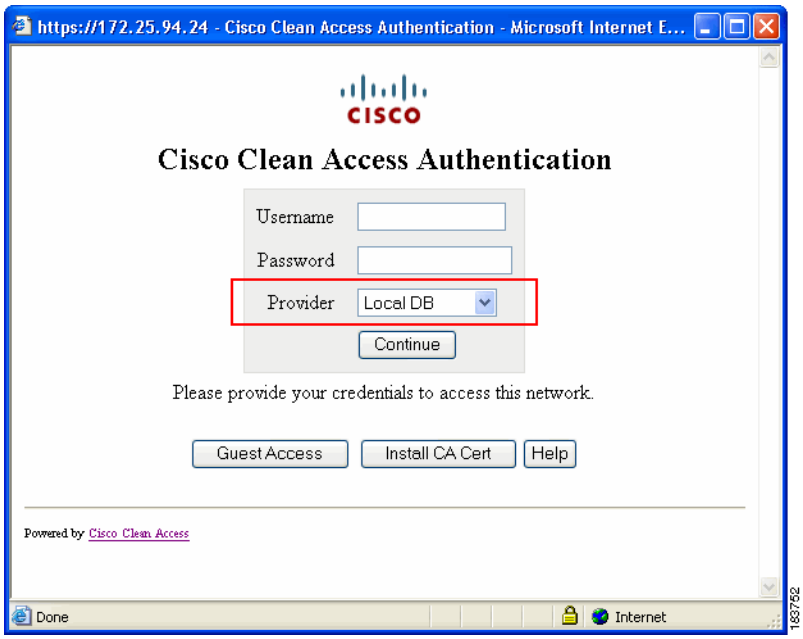
Local Authentication

You can set up any combination of local and external authentication mechanisms for both users and Cisco NAC Appliance administrators. Typically, external authentication sources are used for general users, while local authentication (where users are validated internally to the CAM) is used for test users, guests, or other types of users with limited network access. For details on using local authentication for guest access, see Guest User Access, page 5-17.

Providers

A provider is a configured authentication source. You can configure the providers you set up to appear in the **Provider** dropdown menu of the web login page (Figure 7-2) and Agent to allow users to choose the domain in which to be authenticated.

Figure 7-2 Provider Field in Web Login Page



Mapping Rules

You can set up role assignment for users based on the authentication server. For all auth server types, you can create mapping rules to assign users to roles based on VLAN ID. For LDAP and RADIUS auth servers, you can additionally map users into roles based on attribute values passed from the authentication server.

FIPS 140-2 Compliance

For LDAP over GSSAPI and Kerberos functions with FIPS-compliant CAMs/CASs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

You can configure a FIPS 140-2 compliant external RADIUS Authentication Provider type by setting up a secure IPSec tunnel between your Cisco NAC Appliance system and Cisco ACS 4.x in a Windows environment running Windows Server 2003 or 2008.

Adding an Authentication Provider

The following are the general steps to add an authentication server to the Clean Access Manager:

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** list, choose the authentication provider type.

Step 3 For **Provider Name,** type a name that is unique for authentication providers. If you intend to offer your users the ability to select providers from the login page, be sure to use a name that is meaningful or recognizable for your users, since this name will be used.

Step 4 Choose the **Default Role** (user role) to be assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address. The default role is also assigned in the case that LDAP/RADIUS mapping rules do not result in a successful match.

Step 5 Enter an optional **Description** for the authentication server.

Step 6 Complete the fields specific to the authentication type you chose, as described in the following sections.

Step 7 When finished, click **Add Server**.

The new authentication source appears under **User Management > Auth Servers > List**.

- Click the **Edit** icon next to the auth server to modify settings.
- Click the **Mapping** icon next to the auth server to configure VLAN-based mapping rules for any server type, or attribute-based mapping rules for LDAP, RADIUS, and Cisco VPN SSO auth types.

Specific parameters to add each auth server type are described in the following sections:

- Kerberos, page 7-5
- RADIUS, page 7-6
- Windows NT, page 7-15
- LDAP, page 7-16
- Active Directory Single Sign-On (SS0), page 7-22
- Windows NetBIOS SSO, page 7-22
- Cisco VPN SSO, page 7-24
- Allow All, page 7-26
- Guest, page 7-26

Specific parameters to add each auth server type are described in the following sections:

- Authenticating Against a Backend Active Directory, page 7-28

Note To set a default auth provider for users configure the **Default Provider** option under **Administration > User Pages > Login Page > Edit > Content**. See Chapter 5, "Configuring User Login Page and Guest Access."

Kerberos

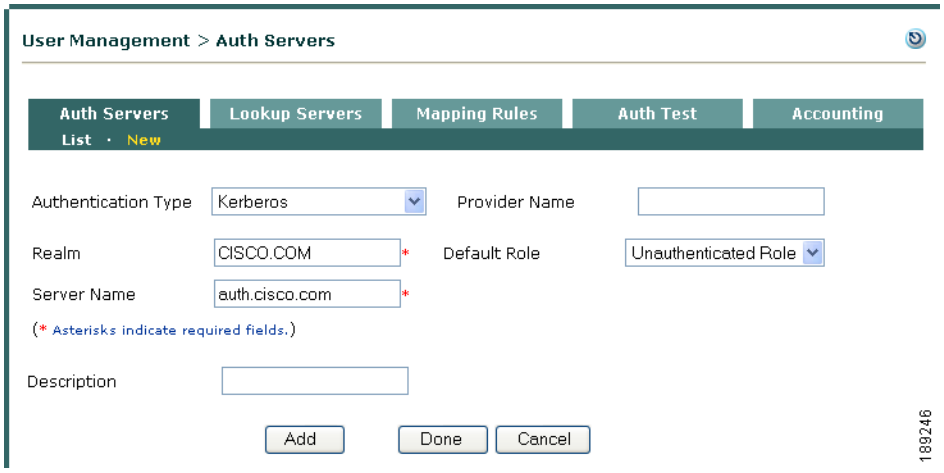
Note In Cisco NAC Appliance, you can configure one Kerberos auth provider and one LDAP auth provider using the GSSAPI authentication method, but only one of the two can be active at any time. See LDAP, page 7-16 for more information.

Note For Kerberos functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **Kerberos**.

Figure 7-3 Add Kerberos Auth Server



Step 3 **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.

Step 4 **Domain Name**—The domain name for your Kerberos realm in UPPER CASE, such as **CISCO.COM**.

Step 5 **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.

Step 6 **Server Name**—The fully qualified host name or IP address of the Kerberos authentication server, such as auth.cisco.com.

Step 7 **Description**—Enter an optional description of this auth server for reference.

Step 8 Click **Add Server.**

Note When working with Kerberos servers, keep in mind that Kerberos is case-sensitive and that the realm name must be in UPPER CASE. The clock must also be synchronized between the CAM and DC.

While running Windows 2008 AD Server at 2003 Server functional level, if you face issues, try the following:

Run KTPass to allow multiple algorithms for new service account.

```
ktpass -princ newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass
PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

Note Before performing the following step, Cisco strongly recommends making a backup copy of the CAM's **/perfigo/control/tomcat/conf/krb.txt** file.

After running the **ktpass** command above, manually modify two files on the CAM as follows:

- In the CAM CLI, navigate to **/perfigo/control/tomcat/conf/krb.txt** and add the following lines:

```
[libdefaults]
   kdc_timeout = 20000
   default_tkt_enctypes = RC4-HMAC
   default_tgs_enctypes = RC4-HMAC
   permitted_enctypes = RC4-HMAC
```

- Navigate to **/perfigo/control/bin/starttomcat**.

  Search for **`CATALINA_OPTS`**.

  Add **`-DKRB_OVERRIDE=true`** to the value of **`CATALINA_OPTS`**.

  For example:

```
Old value: CATALINA_OPTS="-server ..."
New Value: CATALINA_OPTS="-server ... -DKRB_OVERRIDE=true"
```

Note If you are applying this change to an existing HA pair, you must perform the above update on both the HA-Primary and HA-Secondary CAM just as you would upgrade a pair of HA-enabled CAMs. For more information, see the corresponding *Release Notes for Cisco NAC Appliance*.

Restart the CAM by entering the **`service perfigo stop`** and **`service perfigo start`** commands. See also *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for complete details.

RADIUS

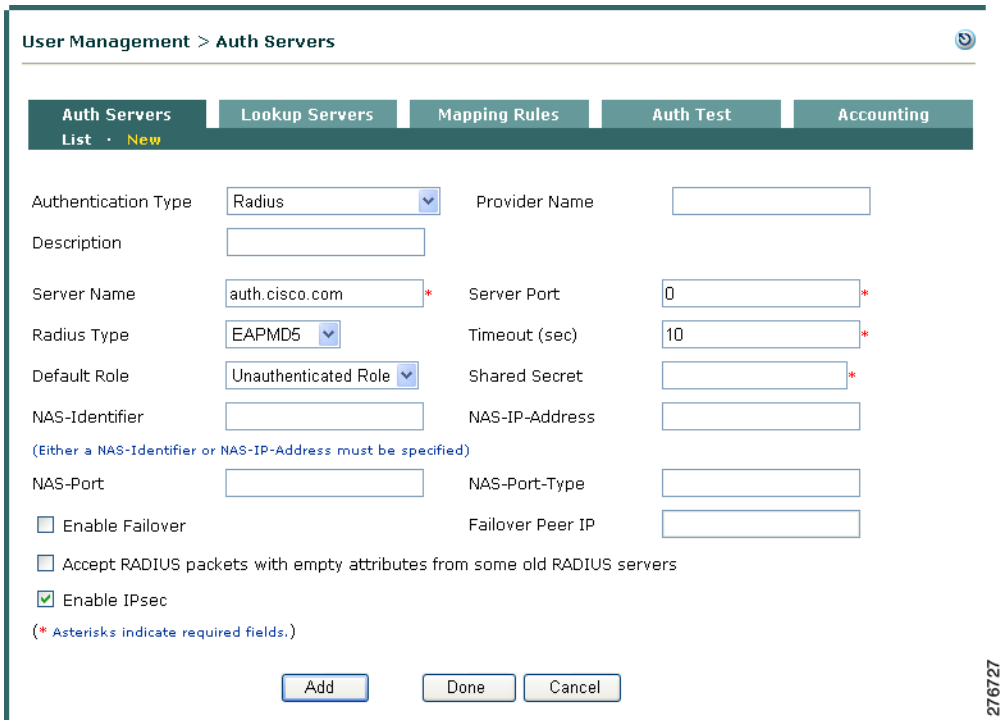
The RADIUS authentication client in the Clean Access Manager can support failover between two RADIUS servers. This allows the CAM to attempt to authenticate against a pair of RADIUS servers, trying the primary server first and then failing over to the secondary server if it is unable to communicate with the primary server. See the **Enable Failover** and **Failover Peer IP** field descriptions below for details.

Note To configure an IPSec tunnel required to connect Cisco NAC Appliance with an external RADIUS server, refer to Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server, page 7-8. This configuration procedure specifies what you need to set up to connect the CAM with an ACS server to perform RADIUS authentication in a FIPS 140-2 compliant network deployment.

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **Radius**.

Figure 7-4 Add RADIUS Auth Server



Step 3 **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.

Step 4 **Server Name**—The fully qualified host name (e.g., auth.cisco.com) or IP address of the RADIUS authentication server.

Step 5 **Server Port**—The port number on which the RADIUS server is listening.

Step 6 **Radius Type**—The RADIUS authentication method. Supported methods include: EAPMD5, PAP, CHAP, MSCHAP, and MSCHAP2.

Step 7 **Timeout (sec)**—The timeout value for the authentication request.

Step 8 **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if RADIUS mapping rules do not result in a successful match.

Step 9 **Shared Secret**—The RADIUS shared secret bound to the specified client's IP address.

Step 10 **NAS-Identifier**—The NAS-Identifier value to be sent with all RADIUS authentication packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.

Step 11 **NAS-IP-Address**—The NAS-IP-Address value to be sent with all RADIUS authentication packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to send the packets.

Note If your CAM is deployed as a member of an HA failover pair, be sure you specify the service IP address for the HA pair to ensure the RADIUS authentication server receives the proper RADIUS accounting packets from the CAM. Regardless of whether the HA-Primary or HA-Standby CAM sends the accounting packets it will show up in the accounting packets as the pair. You must also configure the RADIUS authentication server to accept authentication packets from both the HA-Primary and HA-Secondary CAM eth0 IP addresses to ensure that the RADIUS server accepts the packets regardless of which CAM in the HA pair sends them. This is done in Cisco Secure ACS under AAA Clients.

Step 12 **NAS-Port**—The NAS-Port value to be sent with all RADIUS authentication packets.

Step 13 **NAS-Port-Type**—The NAS-Port-Type value to be sent with all RADIUS authentication packets.

Step 14 **Enable Failover**—This enables sending a second authentication packet to a RADIUS failover peer IP if the primary RADIUS authentication server's response times out.

Step 15 **Failover Peer IP**—The IP address of the failover RADIUS authentication server.

Step 16 **Accept RADIUS packets with empty attributes from some old RADIUS servers**—This option enables the RADIUS authentication client to allow RADIUS authentication responses that are malformed due to empty attributes, as long as the responses contain a success or failure code. This may be required for compatibility with older RADIUS servers.

Step 17 For a FIPS 140-2 compliant deployment, activate the **Enable IPsec** checkbox to ensure you can establish a secure IPsec tunnel for authentication traffic. See also, Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server, page 7-8.

Step 18 **Description**—Enter an optional description of this auth server for reference.

Step 19 Click **Add Server**.

Note If you have configured a RADIUS server, the RADIUS Session Timeout for user login is automatically enabled. The timeout duration therefore occurs on a per user basis, depending on the user profile configured on the RADIUS server. See Session Timer, page 8-15 for more details on timers.

Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server

You can configure a FIPS 140-2 compliant external RADIUS Auth Provider type by setting up IPSec communication between your Cisco NAC Appliance system and Cisco ACS 4.x in a Windows environment running Windows Server 2003 or 2008. There are two primary stages to this task:

- Import Certificates in Windows
- Set Up the IPSec Tunnel

Import Certificates in Windows

Step 1 In Windows, choose **Start > Run** and enter `mmc` to open the certificates console window.

Step 2 Select **File > Add/Remove Snap-in** and click **Add**.

Step 3 Click **Certificates**.

Step 4 Under Console Root, click **Certificates (Local Computer)**. A list of PKI objects appears at the right pane.

Step 5 Go to **Action > All Tasks > Import** and click **Next**.

Step 6 Click **Browse**, select the server certificate, and click **Next**

Step 7 Select **Place all certificates in the following store**.

Step 8 Click **Browse**, specify the appropriate certificate, and click **Next**.

Step 9 Click **Next**.

Step 10 Click **Finish**.

Step 11 After installing the certificate in Windows, verify the certificate by double-clicking on the certificate. The General tab should display "You have a private key that corresponds to this certificate." If not, you can use the following OpenSSL command to convert separate key/certificate files into a single .p12 format:

```
openssl pkcs12 -export -in cert.pem -inkey key.pem -out ACSCert.p12
```

Step 12 Enter any password when prompted.

You will also need to use this password when you import the ACS certificate on in Windows.

Step 13 Ensure that the CA from the CAM and ACS are the same (or that the CAM trusts the ACS CA and vice-versa).

Step 14 Go to **Action > All Tasks > Import** and click **Next**.

Step 15 Click **Browse**, select the root CA certificate, and click **Next**.

Step 16 Select **Place all certificates in the following store**.

Step 17 Click **Browse**, select the "Trusted Root Certification Authorities" folder, and click **Next**.

Step 18 Click **Next**.

Step 19 Click **Finish**.

Set Up the IPSec Tunnel

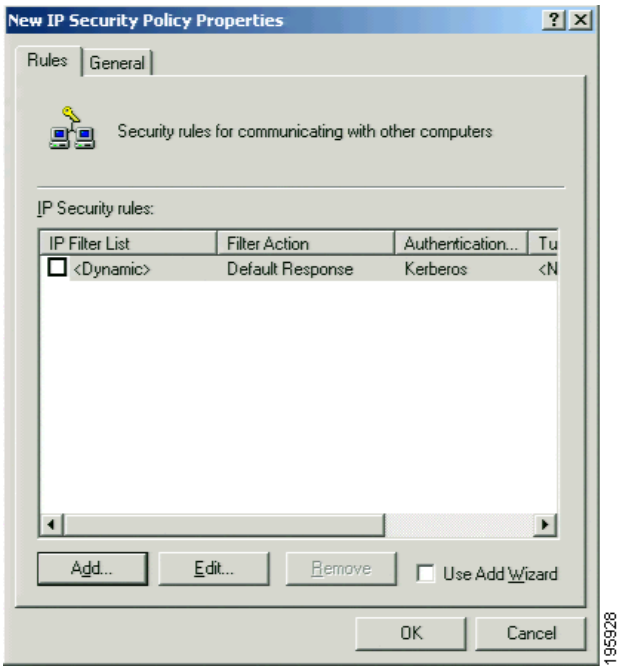
Note Before going through the following procedure, ensure you have disabled the "Use Add Wizard" option for ACS.

Step 1 Go to **Start > Programs > Administrative Tools > Local Security Policy**.

Step 2 Click **IP Security Policies on Local Computer** from the left navigation menu.

Step 3 Go to **Action > Create IP Security Policy** (Figure 7-5).

Figure 7-5 New IP Security Policy



Step 4 On the wizard, click **Next**.

Step 5 Enter a name for the policy (for example, "IPSec rules for CAM-ACS") and click **Next**.

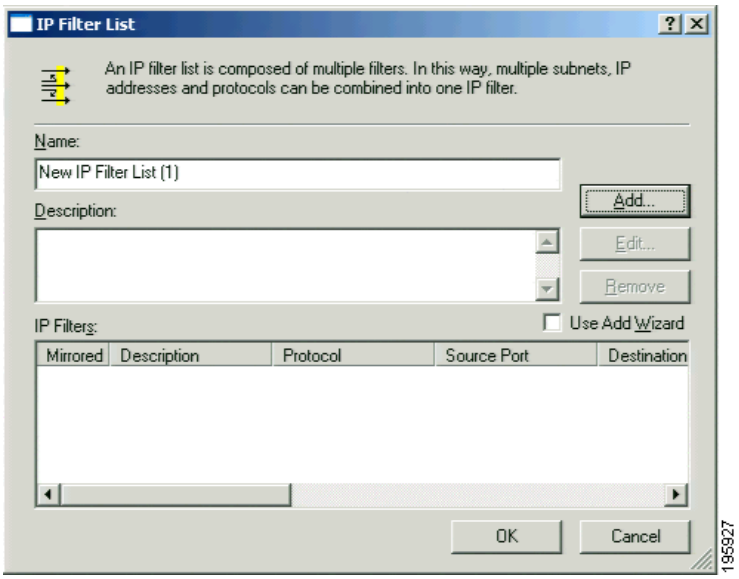
Step 6 Uncheck (disable) the **Activate the default responses rule** option and click **Next**.

Step 7 Leave the **Edit properties** box checked (enabled) and click **Finish**.

Step 8 In the properties dialog, click **Add**.

Step 9 Select the **IP Filter List** tab and click **Add** (Figure 7-6).

Figure 7-6 IP Filter List



Step 10 Specify a name for the IP address filter list (for example, “CAM to ACS Filter List”).

Step 11 Click **Add** to add filter.

Step 12 Select the **Addresses** tab.

Step 13 Specify **A Specific IP address** as the **Source** address and enter the CAM IP address.

Step 14 Specify **A Specific IP address** as the **Destination** address and enter the ACS server IP address.

Step 15 Check (enable) the **Mirrored** option and click **OK**.

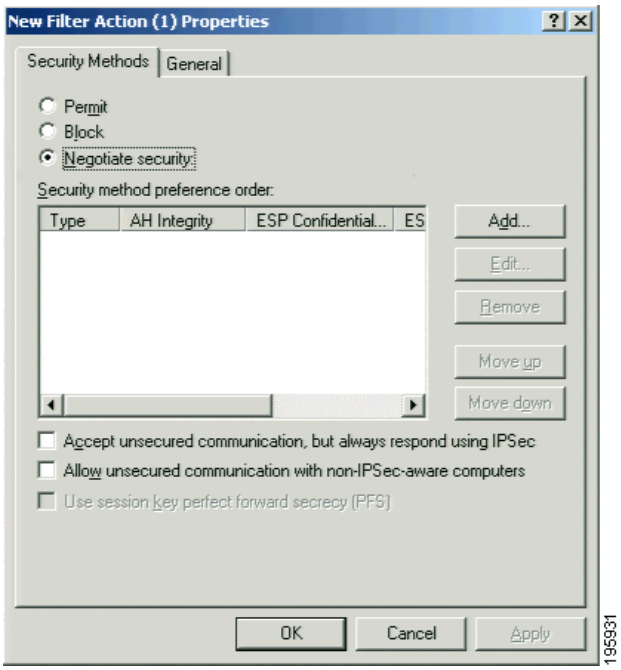
Step 16 If you have deployed your CAMs in an HA configuration, repeat Step 12 through Step 15 for the IP-secondary CAM IP address and service IP address.

Step 17 Click **OK**.

Step 18 In the Filter lists, choose the radio button of the list you just created.

Step 19 Select the **Filter Action** tab and click **Add** to add a new filter action (Figure 7-7).

Figure 7-7 New Filter Action



Step 20 Select the **General** tab and enter a name (for example, "NAC IPSec Filter Action").

Step 21 Select the **Security Methods** tab.

Step 22 Choose the **Negotiate security** option and click **Add**.

Step 23 Specify **Integrity and encryption** as the security method and click **OK**.

Step 24 Ensure that the following settings are defined:

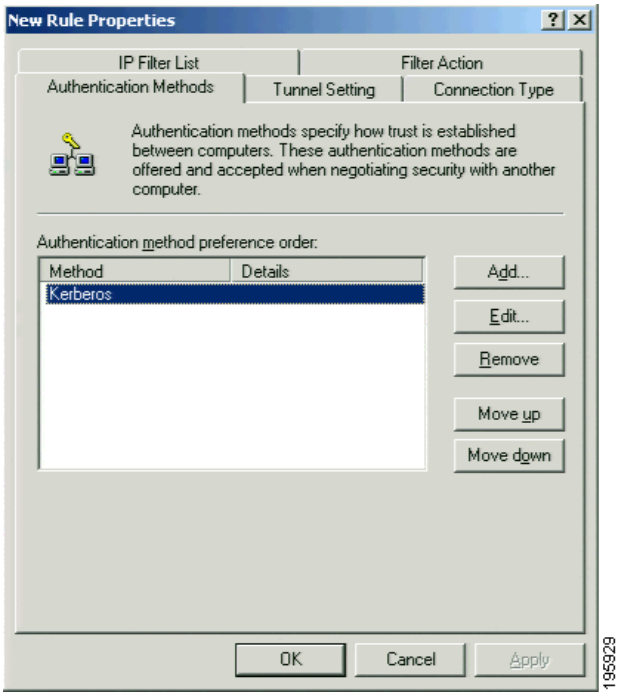
- **AH Integrity** is <*None*>
- **ESP Confidentiality** is **3DES**
- **ESP Integrity** is **SHA1**

Step 25 Check (enable) the **Use session key perfect forward secrecy (PFS)** option and click **OK**.

Step 26 Choose the **NAC IPsec Filter Action** option.

Step 27 Select the **Authentication Methods** tab and remove all authentications methods that are displayed (Figure 7-8).

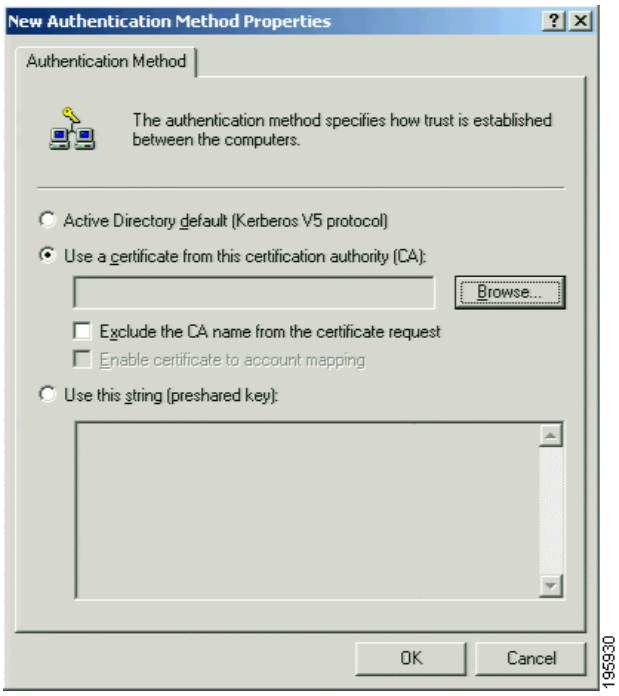
Figure 7-8 Authentication Methods



Step 28 Click **Add**.

Step 29 Select **Use a certificate from this certification authority (CA)** (Figure 7-9).

Figure 7-9 Use a certificate from this certification authority (CA)


New Authentication Method Properties
Authentication Method
The authentication method specifies how trust is established between the computers.
Active Directory default (Kerberos V5 protocol)
Use a certificate from this certification authority (CA):
Browse...
Exclude the CA name from the certificate request
Enable certificate to account mapping
Use this string (preshared key):
OK
Cancel
195930

Step 30 Click **Browse**, select the entry corresponding to your root certificate authority, and click **OK**.

Step 31 Click **OK**.

Step 32 Select the **Tunnel Setting** tab and ensure that the **This rule does not specify and IPSec tunnel** option is specified. This option specifies that the system should use transport mode and not tunnel mode.

Step 33 Select the **Connection Type** tab and ensure that the **All network connections** option is enabled.

Step 34 Click **OK**.

Step 35 Click on the rule you created in the right pane and go to **Action > Assign**.

Step 36 Ping the ACS server IP address from the CAM to ensure they can see on another on the network.

Step 37 Navigate to the **User Management > Auth Servers > Auth Test** CAM web console page and perform an Auth Test for this RADIUS server to verify connectivity, as described in Auth Test, page 7-39.

RADIUS Challenge-Response Impact On the Agent

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the end-user Agent login session can accommodate extra authentication challenge-response dialogs not available in other dialog sessions—beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN

or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session. For details, refer to RADIUS Challenge-Response Cisco NAC Agent Dialogs, page 10-22.

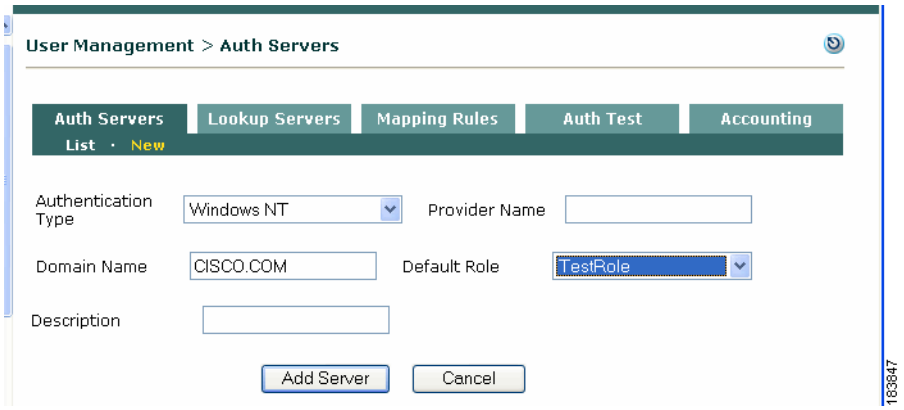
Windows NT

Note

- If the CAM is not in the same subnet as the domain controllers, then the CAM DNS settings must be able to resolve the DCs.
- Currently, only NTLM v1 is supported.

1. Go to **User Management > Auth Servers > New**.
2. From the **Authentication Type** dropdown menu, choose **Windows NT**.

Figure 7-10 Add Windows NT Auth Server



3. **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.
4. **Domain Name**—The host name of the Windows NT environment.
5. **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
6. **Description**—Enter an optional description of this auth server for reference.
7. Click **Add Server**.

LDAP

Note This section describes the general steps to configure an LDAP authentication provider. You can also use these steps to configure SIMPLE or GSSAPI authentication for an LDAP Lookup Server, which is used for authorization when configuring AD SSO. For details on configuring AD SSO, refer to the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

An LDAP auth provider in the Clean Access Manager can be used to authenticate users against a Microsoft Active Directory server. See Authenticating Against a Backend Active Directory, page 7-28 for details. You can configure the LDAP server to use one of two authentication mechanisms:

- **SIMPLE**—The CAM and LDAP server pass user ID and password information between themselves without encrypting the data. See Configure LDAP Server with Simple Authentication, page 7-17.
- **GSSAPI**—(Generic Security Services Application Programming Interface) Provides an option to encrypt user ID and password information passed between the CAM and the specified LDAP server to help ensure privacy. See Configure LDAP Server with GSSAPI Authentication, page 7-18.

Note To ensure complete DNS capability when using GSSAPI, you must ensure that all Domain Controllers, child domains, and hosts conform to strict DNS naming conventions and that you have the ability to perform both forward- and reverse-DNS.

In Cisco NAC Appliance, you can configure one LDAP auth provider using the GSSAPI authentication method and one Kerberos auth provider, but only one of the two can be active at any time. See Kerberos, page 7-5 for more information.

For LDAP over GSSAPI functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

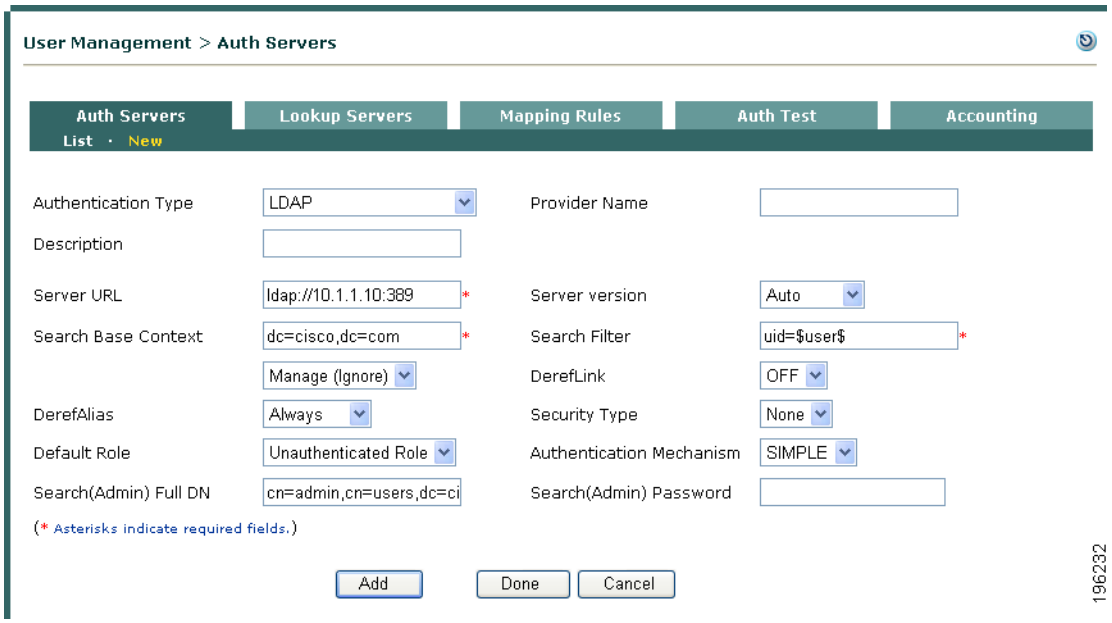
Note Cisco NAC Appliance performs standard search and bind authentication. For LDAP, if Search(Admin) Username/Search(Admin) Password is not specified, Cisco NAC Appliance attempts anonymous bind.

Configure LDAP Server with Simple Authentication

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **LDAP**.

Figure 7-11 Add LDAP Auth Server—SIMPLE Authentication Mechanism



Step 3 **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.

Step 4 **Description**—Enter an optional description of this auth server for reference.

Step 5 **Server URL**—Type the URL of the LDAP server, in the form:

```
ldap://<directory_server_name>:<port_number>
```

If no port number is specified, 389 is assumed.

Note When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments.

You can add redundancy for LDAP Authentication servers by entering multiple LDAP URLs in the Server URL field separated by a space, for example:

```
ldap://ldap1.abc.com ldap://ldap2.abc.com ldap://ldap3.abc.com
```

If the first LDAP server listed does not respond within 15 seconds, the CAM then attempts to authenticate using the alternate LDAP server(s) in the list. Every LDAP authentication request is passed to the first server specified in the list by default. You can only input 128 characters in this field, thus limiting the number of redundant servers you can specify.

Step 6 **Server version**—The LDAP version. Supported types include Version 2 and Version 3. Leave as **Auto** (default) to have the server version automatically detected.

Step 7 **Search Base Context**—The root of the LDAP tree in which to perform the search for users (e.g. dc=cisco, dc=com).

Step 8 **Search Filter**—The attribute to be authenticated (e.g., uid=$user$, or sAMAccountName=$user$).

Step 9 **Referral**—Whether referral entries are managed (in which the LDAP server returns referral entries as ordinary entries) or returned as handles (Handle(Follow)). The default is Manage(Ignore).

Step 10 **DerefLink**—If **ON**, object aliases returned as search results are de-referenced, that is, the actual object that the alias refers to is returned as the search result, not the alias itself. The default is OFF.

Step 11 **DerefAlias**—Options are Always (default), Never, Finding, Searching.

Step 12 **Security Type**—Whether the connection to the LDAP server uses SSL. The default is None.

Note If the LDAP server uses SSL, be sure to import the certificate using the **Import Certificate** option on the **Administration > CCA Manager > SSL > X509 Certificate** page.

Step 13 **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if LDAP mapping rules do not result in a successful match.

Step 14 Specify the **Authentication Mechanism** to be **SIMPLE**.

Step 15 **Search(Admin) Full DN**—The Search(Admin) user can be an LDAP administrator or a basic user. If using LDAP to connect to an AD server, the Search(Admin) Full DN (distinguished name) must be the DN of an AD user account and the first CN (common name) entry should be an AD user with read privileges. (See Figure 7-11.)

```
cn= jane doe, cn=users, dc=cisco, dc=com
```

Step 16 **Search(Admin) Password**—The password for the LDAP user.

Step 17 Click **Add Server**.

Configure LDAP Server with GSSAPI Authentication

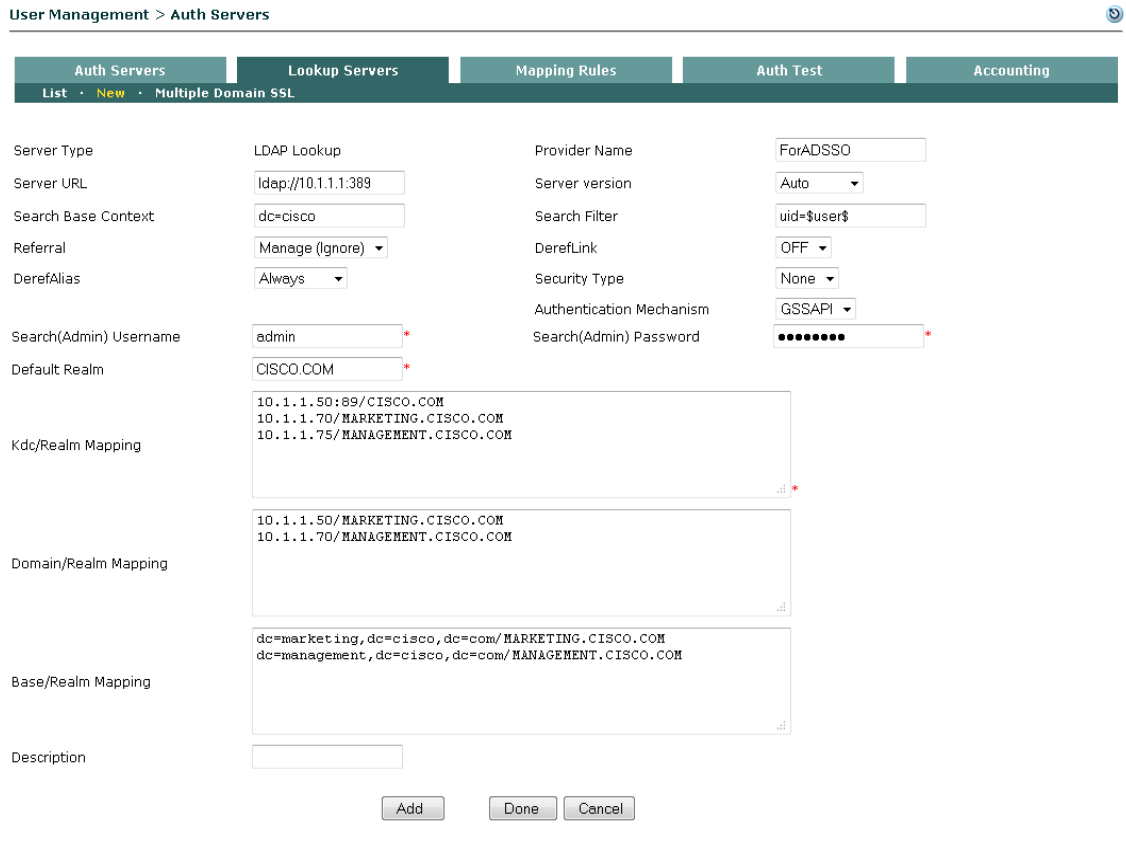
Note In Cisco NAC Appliance, you can configure one LDAP auth provider using the GSSAPI authentication method and one Kerberos auth provider, but only one of the two can be active at any time. See Kerberos, page 7-5 for more information.

Note For LDAP over GSSAPI functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

Step 1 Go to **User Management > Auth Servers > Lookup Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **LDAP**.

Figure 7-12 Add LDAP Auth Server—GSSAPI Authentication Mechanism



Step 3 **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.

Step 4 **Description**—Enter an optional description of this auth server for reference.

Step 5 **Server URL**—Type the URL of the LDAP server, in the form:

```
ldap://<directory_server_name>:<port_number>
```

If no port number is specified, 389 is assumed.

Note When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments.

You can add redundancy for LDAP Authentication servers by entering multiple LDAP URLs in the Server URL field separated by a space, for example:

```
ldap://ldap1.abc.com ldap://ldap2.abc.com ldap://ldap3.abc.com
```

If the first LDAP server listed does not respond within 15 seconds, the CAM then attempts to authenticate using the alternate LDAP server(s) in the list. Every LDAP authentication request is passed to the first server specified in the list by default. You can only input 128 characters in this field, thus limiting the number of redundant servers you can specify.

Step 6 **Server version**—The LDAP version. Supported types include Version 2 and Version 3. Leave as **Auto** (default) to have the server version automatically detected.

Step 7 **Search Base Context**—The root of the LDAP tree in which to perform the search for users (e.g. dc=cisco, dc=com).

Step 8 **Search Filter**—The attribute to be authenticated (e.g., uid=$user$, or sAMAccountName=$user$).

Step 9 **Referral**—Whether referral entries are managed (in which the LDAP server returns referral entries as ordinary entries) or returned as handles (Handle(Follow)). The default is Manage(Ignore).

Step 10 **DerefLink**—If **ON**, object aliases returned as search results are de-referenced, that is, the actual object that the alias refers to is returned as the search result, not the alias itself. The default is OFF.

Step 11 **DerefAlias**—Options are Always (default), Never, Finding, Searching.

Step 12 **Security Type**—Whether the connection to the LDAP server uses SSL. The default is None.

Note If the LDAP server uses SSL, be sure to import the certificate using the **Import Certificate** option on the **Administration > CCA Manager > SSL > X509 Certificate** page.

If you choose SSL, ensure that you provide the details in the Multiple Domain SSL tab as well. See Multiple Domain SSL, page 7-21.

Step 13 **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if LDAP mapping rules do not result in a successful match.

Step 14 Specify the **Authentication Mechanism** to be **GSSAPI**.

Note For LDAP over GSSAPI functions with FIPS 140-2 compliant CAMs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

Step 15 **Search(Admin) Username**—If access to the directory is controlled, this field is automatically populated with the LDAP user ID used to connect to the server ("admin" in the example illustrated in Figure 7-12).

Step 16 **Search(Admin) Password**—The password for the LDAP user.

Step 17 **Default Realm**—The realm with which the LDAP server is most commonly associated.

Step 18 **KDC Timeout (in seconds)**—The period of time the CAM keeps trying to connect before declaring the specified KDC server unreachable.

Step 19 **KDC/Realm Mapping**—You can specify one or more mappings between LDAP server IP address/port specifications and LDAP realms.

Note You can also specify "failover" or "redundant" mappings in the **KDC/Realm Mapping** field. For example, if you specify an LDAP server IP address-to-realm mapping, but use a redundant LDAP server in your network, you can also enter the backup LDAP server's IP address immediately after the primary IP address-to-realm mapping to ensure the CAM also checks with the redundant server in case the first one is unreachable.

Step 20 **Domain/Realm Mapping**—You can specify one or more mappings between LDAP server domains and LDAP realms.

Step 21 **Base/Realm Mapping**—You can specify a different LDAP Search Base depending on which Kerberos Realm is being authenticated.

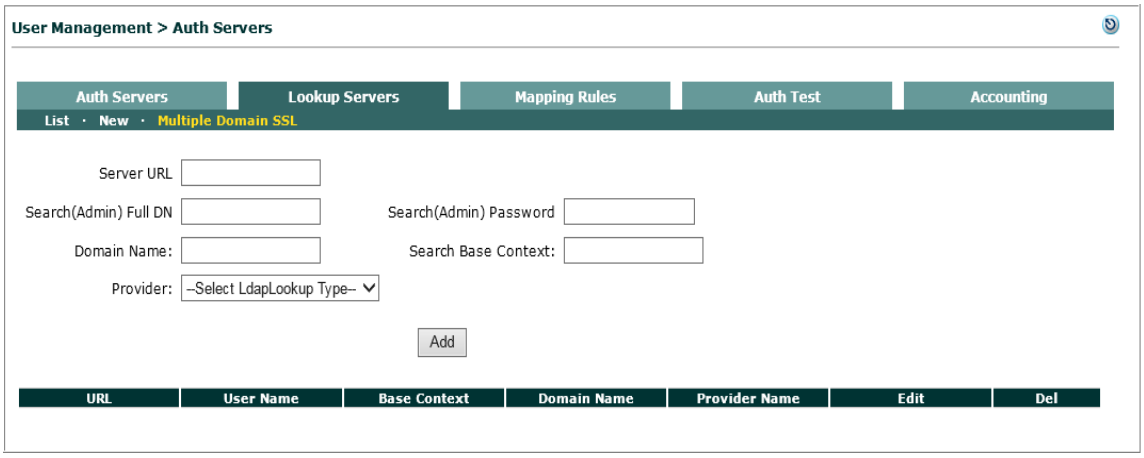
Step 22 Click **Add Server**.

Multiple Domain SSL

When you choose the LDAP server to use SSL, you need to provide the details in the Multiple Domain SSL tab as well.

Step 1 Go to **User Management > Auth Servers > Lookup Servers > Multiple Domain SSL**.

Figure 7-13 Multiple Domain SSL



Step 2 Choose the appropriate LDAP provider name from the **Provider** drop-down.

Step 3 Enter the other details according to the provider you have selected as follows:

a. **Server URL**—Type the URL of the LDAP server, in the form:

```
ldap://<directory_server_name>:<port_number>
```

If no port number is specified, 389 is assumed.

b. **Search(Admin) Full DN**—Enter the distinguished name(DN) of an AD user account and the first CN (common name) entry should be an AD user with read privileges.

c. **Domain Name**—Enter the domain name for your LDAP server in upper case, such as CISCO.COM.

d. **Search(Admin) Password**—The password for the LDAP user.

e. **Search Base Context**—The root of the LDAP tree to perform the search for users (e.g. dc=cisco, dc=com).

Step 4 Click **Add**.

Step 5 The bottom pane displays the details of the servers you have added.

Step 6 You can click the Edit icon to modify the details and the Delete icon to remove a server.

Note If a domain has child domains, you must add the server details for each child domain separately.

Active Directory Single Sign-On (SSO)

See the "Configuring Active Directory Single Sign-On (AD SSO)" chapter in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for complete details.

Windows NetBIOS SSO

Note The Windows NetBIOS SSO authentication feature is deprecated. Cisco recommends the "Configuring Active Directory Single Sign-On (AD SSO)" chapter in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* instead.

In Windows NetBIOS SSO authentication (formerly known as "Transparent Windows"), the CAS sniffs relevant Windows login packets from the end-user machine to the domain controller to determine whether or not the user is logged in successfully. If Windows NetBIOS SSO authentication is enabled and the CAS successfully detects login traffic, the user is logged into the Cisco NAC Appliance system without having to explicitly login through the web login page or Agent.

With Windows NetBIOS SSO, only authentication can be done—posture assessment, quarantining, remediation, do not apply. However, the user only needs to perform Ctrl-Alt-Dlt to login.

Note For Windows NetBIOS SSO login, it is not required for the CAM to be on the same subnet as the domain controller. The list of Windows NetBIOS SSO DC is published from the CAM.

Implementing Windows NetBIOS SSO

Implementing Windows NetBIOS SSO login involves the following steps:

1. Add a **Windows NetBIOS SSO** auth server through **User Management > Auth Servers > New Server** (see Add Windows NetBIOS SSO Auth Server, page 7-23).
2. From **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > NetBIOS SSO**:
   a. Click the option for **Enable Transparent Windows Single Sign-On with NetBIOS** on the specific CAS and click **Update**.

b. Enter each **Windows Domain Controller IP** and click **Add Server**.

See section "Enable Windows NetBIOS SSO" of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

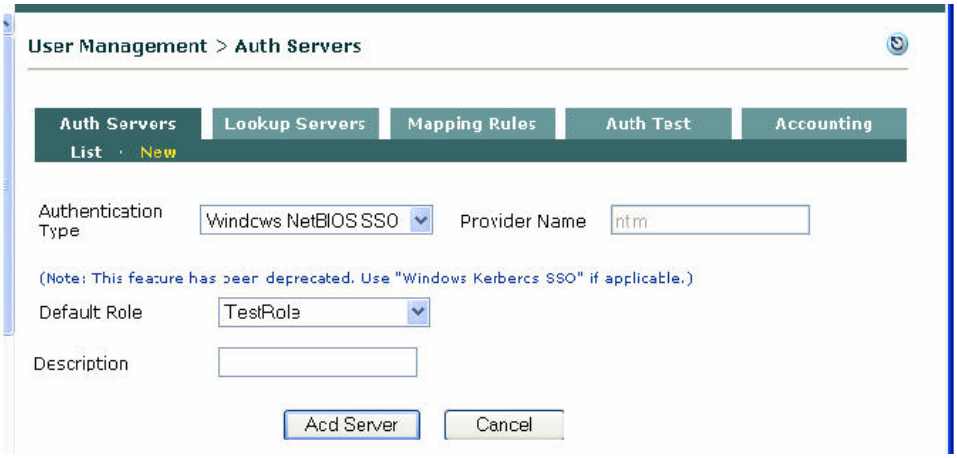
3. Add IP traffic control policies for the Unauthenticated role to allow users on the untrusted side access to the domain controllers on the trusted network. Typical policies may include allowing TCP, and UDP traffic for each controller (IP address and 255.255.255.255 mask) for ports 88(Kerberos), 135 (DCE endpoint resolution), 139 (netbios-ssn), 389 (LDAP), 445(smb-tcp). See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule."

Note Because the CAS attempts to authenticate the user by sniffing Windows logon packets on the network, if the end device does not send such traffic (i.e. authenticates from cache) the CAS cannot authenticate the user. In order to cause such login traffic to be generated, you can use a login script to establish network shares/shared printers. You can also login as a different user from the same machine to cause the machine to communicate to the domain controller (typically a different user's credentials will not be cached).

Add Windows NetBIOS SSO Auth Server

1. Go to **User Management > Auth Servers > New Server**.
2. From the **Authentication Type** dropdown menu, choose **Windows NetBIOS SSO**.

Figure 7-14 Add Windows NetBIOS SSO Auth Server



3. **Provider Name**—The **Provider Name** value defaults to **ntlm**.
4. **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.
5. **Description**—Enter an optional description of this auth server for reference.
6. Click **Add Server**.

Cisco VPN SSO

Cisco NAC Appliance enables administrators to deploy the CAS In-Band behind a VPN concentrator, or router, or multiple routers. Cisco NAC Appliance supports multi-hop Layer 3 In-Band deployment by allowing the CAM and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. With Layer 2-connected users, the CAM/CAS continue to manage these user sessions based on the user MAC addresses, as before.

Note Cisco NAC Appliance supports Single Sign-On (SSO) for the following:

- Cisco VPN Concentrators
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Airespace Wireless LAN Controllers
- Cisco SSL VPN Client (Full Tunnel)
- Cisco VPN Client (IPSec)

You can configure Cisco NAC Appliance to perform VPN SSO via a Cisco ASA in a FIPS-compliant network deployment. For detailed configuration information, see the "Configure VPN SSO in a FIPS 140-2 Compliant Deployment" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Cisco NAC Appliance provides integration with Cisco VPN concentrators and can enable SSO capability for VPN users, using RADIUS Accounting information. The Clean Access Server can acquire the client's IP address from either Framed_IP_address or Calling_Station_ID RADIUS attributes for SSO purposes.

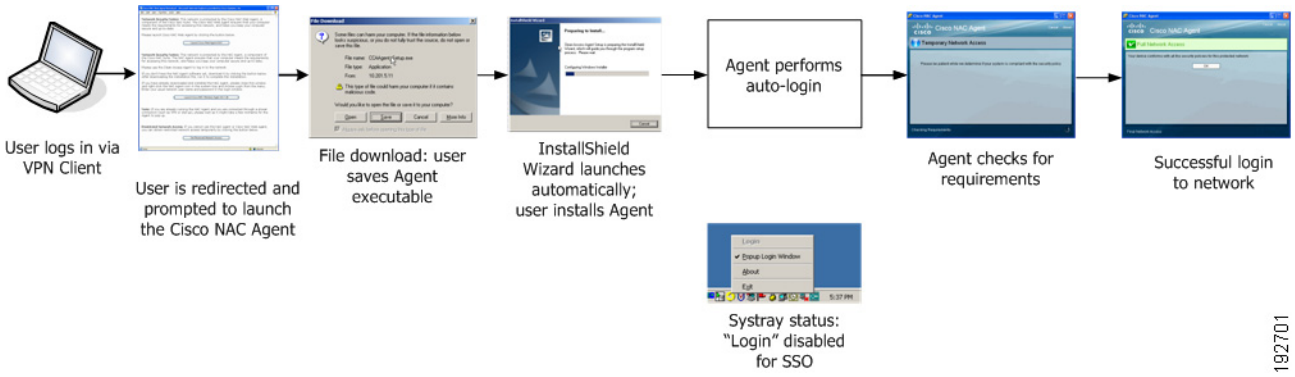
- Single Sign-On (SSO) for Cisco VPN concentrator users—VPN users do not need to login to the web browser or the Agent because the RADIUS accounting information sent to the CAS/CAM by the VPN concentrator provides the user ID and IP address of users logging into the VPN concentrator (RADIUS Accounting Start Message).

  Note A CAS deployed as a Real-IP gateway supporting VPN SSO opens the Accounting port only on the trusted (eth0) interface. For configuration information, see the "Integrating with Cisco VPN Concentrators" chapter of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

- Single Sign-On (SSO) for Cisco Airespace Wireless LAN Controller users—For SSO to work, the Cisco Airespace Wireless LAN Controller must send the Calling_Station_IP attribute as the client's IP address (as opposed to the Framed_IP_address that the VPN concentrator uses).
- Accurate Session Timeout/Expiry—Due to the use of RADIUS accounting, the VPN concentrator informs the Clean Access Server exactly when the user has logged out (RADIUS Accounting Stop Message). See OOB (L2) and Multihop (L3) Sessions, page 8-16 for additional details.

Figure 7-15 illustrates the login and posture assessment process for a VPN user using the Agent with Single Sign-On. Note that the initial download of the Agent must be performed via the VPN connection.

Figure 7-15 Agent with SSO for VPN Users


User logs in via VPN Client
User is redirected and prompted to launch the Cisco NAC Agent
File download: user saves Agent executable
InstallShield Wizard launches automatically; user installs Agent
Agent performs auto-login
Agent checks for requirements
Successful login to network
Systray status: "Login" disabled for SSO
192701

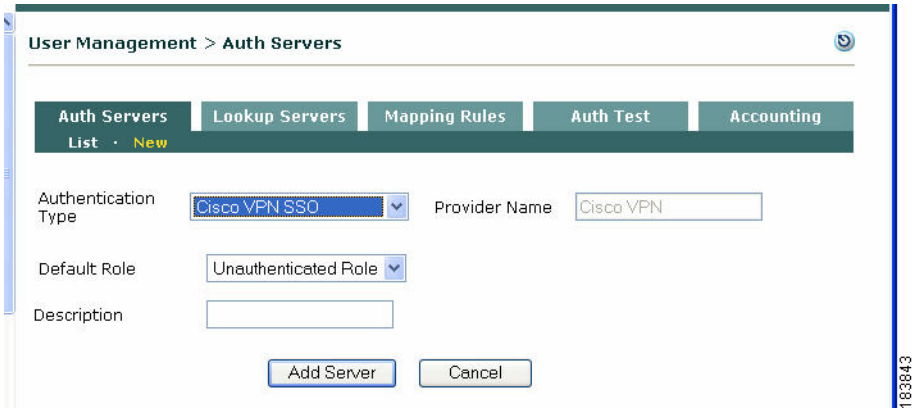
Add Cisco VPN SSO Auth Server

To enable SSO for Cisco VPN concentrator users, add a Cisco VPN SSO auth server:

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **Cisco VPN SSO**.

Figure 7-16 Add Cisco VPN Auth Server



Step 3 **Provider Name**—The **Provider Name** value defaults to **CiscoVPN**.

Step 4 **Default Role**—Choose the user role assigned to users authenticated by the Cisco VPN concentrator. This default role is used if not overridden by a role assignment based on MAC address or IP address, or if RADIUS mapping rules do not result in a successful match.

Step 5 **Description**—Enter an optional description of the Cisco VPN concentrator for reference.

Step 6 Click **Add Server**.

Make sure you have completed configuration under **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth**. For complete details on configuring the Clean Access Server for VPN concentrators, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Allow All

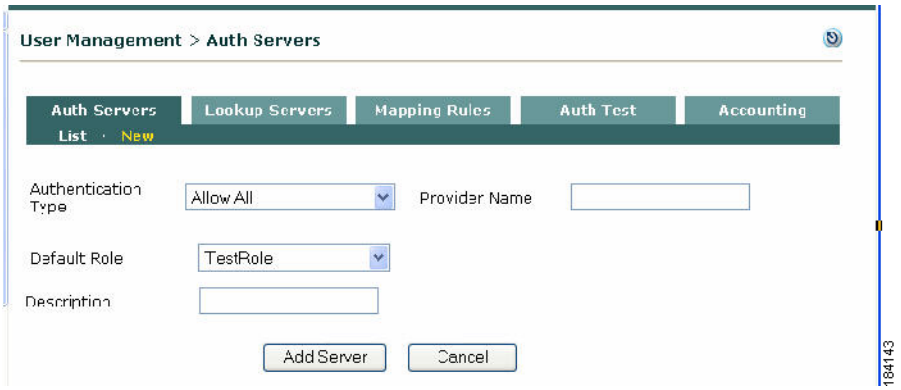
The **AllowAll** option is a special authentication type that provides an alternative to the Guest Access login button feature. It allows users to type in any credential to login (e.g., an email address for user name and/or password) but does not validate the credentials. This option can be used when administrators want to capture limited information on who is logging in (such as a list of email addresses). The identifier the user submits in the login page will appear as the **User Name** in the Online Users page while the user is logged in. In this case, administrators should also modify the **Username Label** button label on the login page to reflect the type of value they want users to enter as a credential. See Guest User Access, page 5-17 for additional details.

Note The AllowAll auth type can be applied to users other than "guest." Any normal login role (e.g. one configured for posture assessment) can be specified as the Default Role for the AllowAll auth type.

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **Allow All**.

Figure 7-17 Allow All Auth Server Type



Step 3 **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.

Step 4 **Default Role**—Choose the user role assigned to users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address.

Step 5 **Description**—Enter an optional description of this auth server for reference.

Step 6 Click **Add Server**.

Guest

The **Guest** option is very similar in implementation and application to the **Allow All** auth server type and it serves as a useful alternative to guest users simply logging in via the existing guest access button on the web login page. Like the **Allow All** auth server type, the **Guest** option allows users to type in any credential to login (e.g., an Email address for user name and/or password) but does not validate the credentials, but also enables you to collect other required or optional information not available in the

Allow All function. For example, you can require users to supply a contact phone number and birth date before they are allowed to access the network as a guest user. The identifier a user submits in the login page appears in the **Online Users** and **User Management > Local Users > Guest Users** pages while the user is logged in.

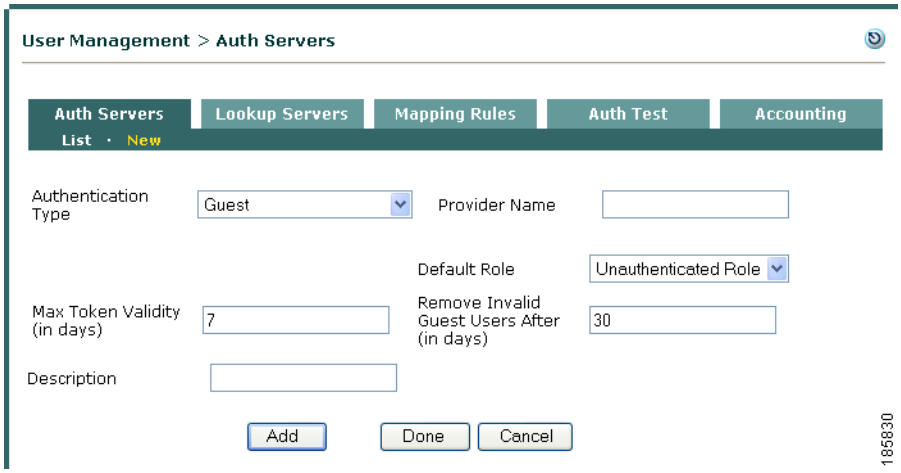
Note You can only configure one "Guest" Auth Server type in the Cisco NAC Appliance system at a time.

To configure a Guest authentication server type:

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **Guest**.

Figure 7-18 Guest Auth Server Type



Step 3 **Provider Name**—Type a unique name for this authentication provider. Enter a meaningful or recognizable name if web login users will be able to select providers from the web login page.

Step 4 **Default Role**—Choose the user role assigned to guest users authenticated by this provider. This default role is used if not overridden by a role assignment based on MAC address or IP address. The default value is 30 days.

Step 5 **Max Token Validity (in days)**—Enter the number of days a guest user account remains valid in the NAC Appliance system. The default value is 7 days.

Step 6 **Remove Invalid Guest Users After (in days)**—Once a guest user account has been "Invalid" for the specified number of days, the NAC Appliance system reserves the right to remove that guest user account from the NAC Appliance system database.

Tip If your NAC Appliance system provides guest access to a very large number of different guest users on a regular basis, you might want to consider changing the **Remove Invalid Guest Users After (in days)** setting to a smaller number to help minimize the number of invalid/legacy user IDs in the database.

Step 7 **Description**—Enter an optional description of this guest authentication server for reference.

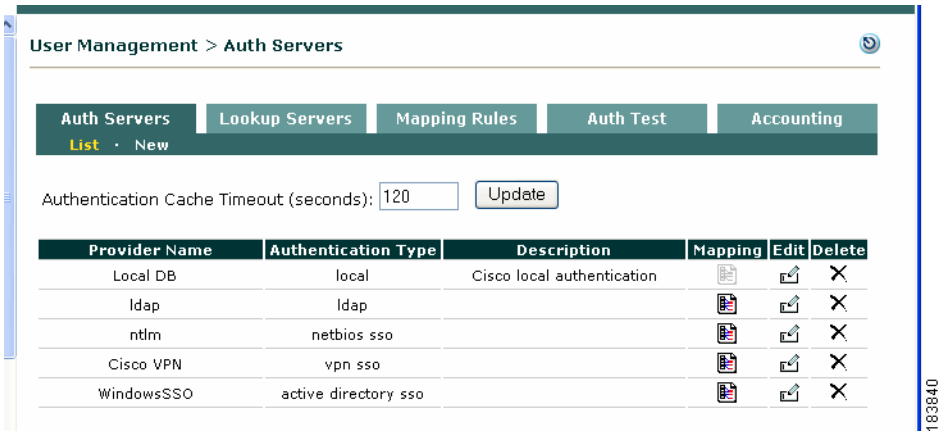
Step 8 Click **Add Server**.

Configuring Authentication Cache Timeout (Optional)

For performance reasons, the Clean Access Manager caches the authentication results from user authentication for 2 minutes by default. The **Authentication Cache Timeout** control on the Auth Server list page allows administrators to configure the number of seconds the authentication result will be cached in the CAM. When a user account is removed from the authentication server (LDAP, RADIUS, etc.), administrators can restrict the time window a user can login again into Cisco NAC Appliance by configuring the Authentication Cache Timeout.

Step 1 Go to **User Management > Auth Servers > Auth Servers > List**.

Figure 7-19 List Auth Servers



Step 2 Type the number of seconds you want user authentication results to be cached in the CAM. The default is 120 seconds; minimum is 1 second, maximum is 86400 seconds.

Note If you set this timeout value to 0, the CAM does not cache user authentication results although this method may affect performance due to increased authentication traffic for multiple users logging into Cisco NAC Appliance.

Step 3 Click **Update**.

Authenticating Against a Backend Active Directory

Several types of authentication providers in the Clean Access Manager can be used to authenticate users against an Active Directory server, Microsoft's proprietary directory service. These include Windows NT (NTLM), Kerberos, and LDAP (preferred).

If using LDAP to connect to the AD server, the **Search(Admin) Full DN** (distinguished name) can be the DN of an AD administrator or user account and the first CN (common name) entry should be an AD user with read privileges.

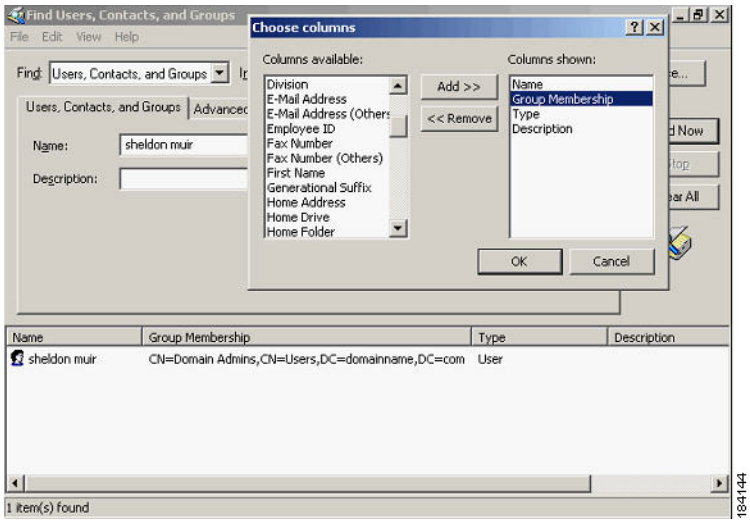
Note The search filter, "sAMAccountName," is the user login name in the default AD schema.

AD/LDAP Configuration Example

The following illustrates a sample configuration using LDAP to communicate with the backend Active Directory:

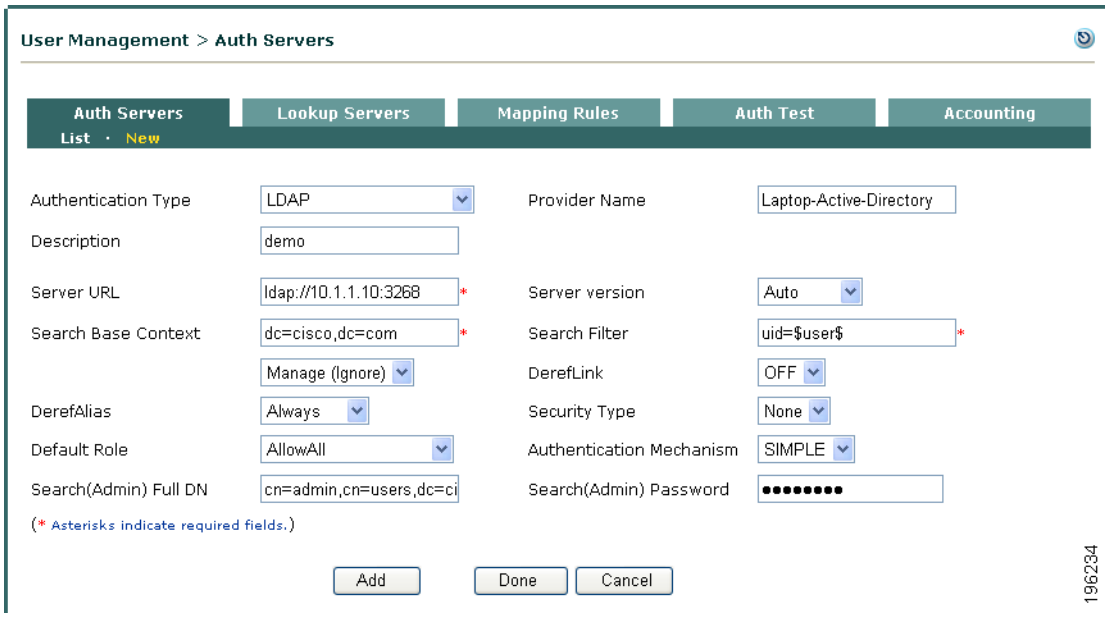
1. Create a Domain Admin user within Active Directory Users and Computers. Place this user into the Users folder.
2. Within Active Directory Users and Computers, select Find from the Actions menu. Make sure that your results show the Group Membership column for the created user. Your search results should show the user and the associated Group Membership within Active Directory. This information is what you will need to transfer into the Clean Access Manager.

Figure 7-20 Find Group Membership within Active Directory



3. From the Clean Access Manager web console, go to the **User Management > Auth Servers > New Server** form.
4. Choose **LDAP** as the **Server Type**.
5. For the **Search(Admin) Full DN** and **Search Base Context** fields, input the results from the Find within Active Directory Users and Computers.

Figure 7-21 Example New LDAP Server for AD



6. The following fields are all that is necessary to properly set up this auth server within the CAM:
   a. **Description**: Used just for reference.
   b. **ServerURL**: ldap://192.168.137.10:3268 – This is the domain controller IP address and default Microsoft Global Catalog port for AD.

Note When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments.

   c. **Search(Admin) Full DN**: CN=sheldon muir, CN=Users, DC=domainname, DC=com
   d. **Search Base Context**: DC=domainname, DC=com
   e. **Default Role**: Select the default role a user will be put into once authenticated.
   f. **Provider Name**: This is the name of the LDAP server used for User Page setup on the CAM.
   g. **Search Password**: sheldon muir's domain password
   h. **Search Filter**: SAMAccountName=$user$
7. Click **Add Server**.
8. At this point, an authentication test using the **Auth Test** feature should work (see Auth Test, page 7-39).

Note You can also use an LDAP browser (e.g. http://www.tucows.com/preview/242937) to validate your search credentials first.

Map Users to Roles Using Attributes or VLAN IDs

The **Mapping Rules** forms can be used to map users into user role(s) based on the following parameters:

- The VLAN ID of user traffic originating from the untrusted side of the CAS (all auth server types)

Note Only Layer 2 Adjacency mode is supported.

- Authentication attributes passed from LDAP and RADIUS auth servers (and RADIUS attributes passed from Cisco VPN Concentrators)

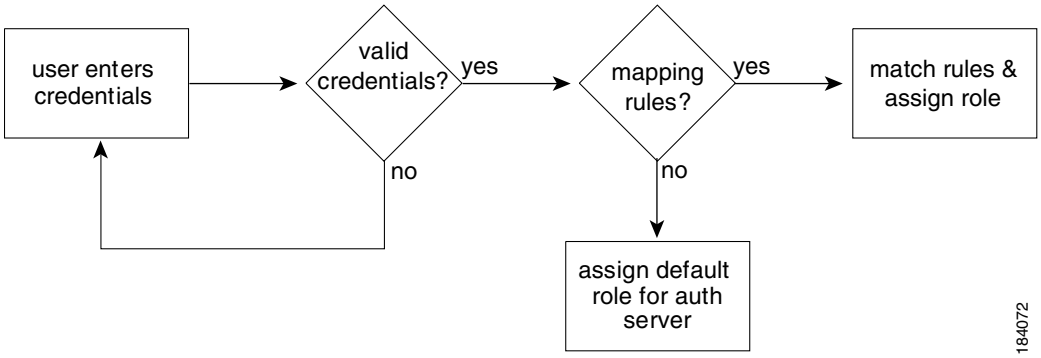
Note You cannot reliably use the "memberOf" attribute to determine the user's Primary Group in an LDAP Active Directory group membership query. You must use a workaround method to be able to map the user's Primary Group VLAN ID, based on Active Directory group membership.

For more information, see the following Microsoft Knowledge Base articles:
http://support.microsoft.com/kb/275523
http://support.microsoft.com/kb/321360

For example, if you have two sets of users on the same IP subnet but with different network access privileges (e.g. wireless employees and students), you can use an attribute from an LDAP server to map one set of users into a particular user role. You can then create traffic policies to allow network access to one role and deny network access to other roles. (See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" for details on traffic policies.)

Cisco NAC Appliance performs the mapping sequence as shown in Figure 7-22.

Figure 7-22 Mapping Rules



Note For an overview of how mapping rules fit into the scheme of user roles, see Figure 6-1Normal Login User Roles, page 6-3.

Cisco NAC Appliance allows the administrator to specify complex Boolean expressions when defining mapping rules for Kerberos, LDAP and RADIUS authentication servers. Mapping rules are broken down into conditions and you can use Boolean expressions to combine multiple user attributes and multiple

VLAN IDs to map users into user roles. Mapping rules can be created for a range of VLAN IDs, and attribute matches can be made case-insensitive. This allows multiple conditions to be flexibly configured for a mapping rule.

A mapping rule comprises an auth provider type, a rule expression, and the user role into which to map the user. The rule expression comprises one or a combination of conditions the user parameters must match to be mapped into the specified user role. A condition is comprised of a condition type, a source attribute name, an operator, and the attribute value against which the particular attribute is matched.

To create a mapping rule you first add (save) conditions to configure a rule expression, then once a rule expression is created, you can add the mapping rule to the auth server for the specified user role.

Mapping rules can be cascading. If a source has more than one mapping rule, the rules are evaluated in the order in which they appear in the mapping rules list. The role for the first positive mapping rule is used. Once a rule is met, other rules are not tested. If no rule is true, the default role for that authentication source is used.

Configure Mapping Rule

1. Do one of the following:

- Go to **User Management > Auth Servers > Mapping Rules** and click the **Add Mapping Rule** link for the authentication server,
- Click the **Mapping** icon for the auth server under **User Management > Auth Servers > List** (Figure 7-23), then click the **Add Mapping Rule** link for the auth server (Figure 7-24).

Figure 7-23 List of Auth Servers

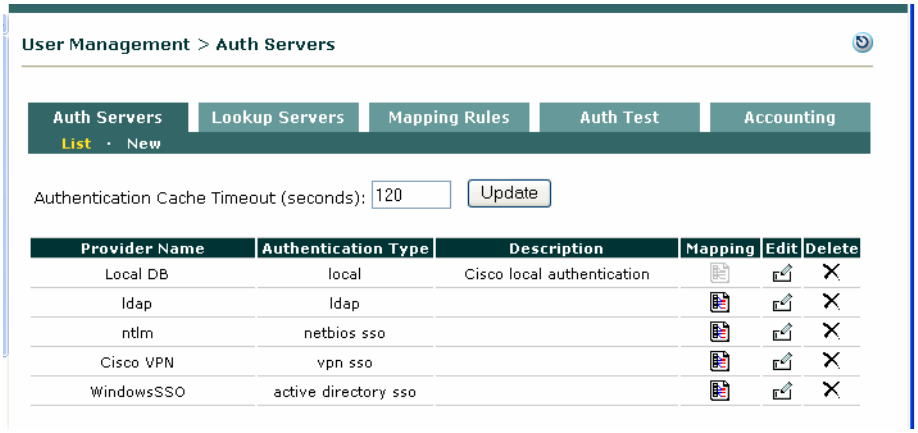
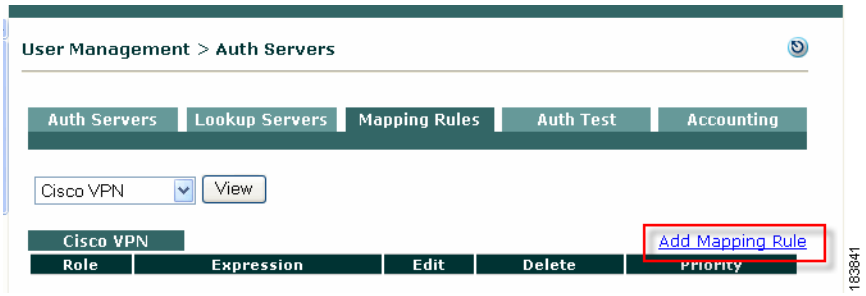
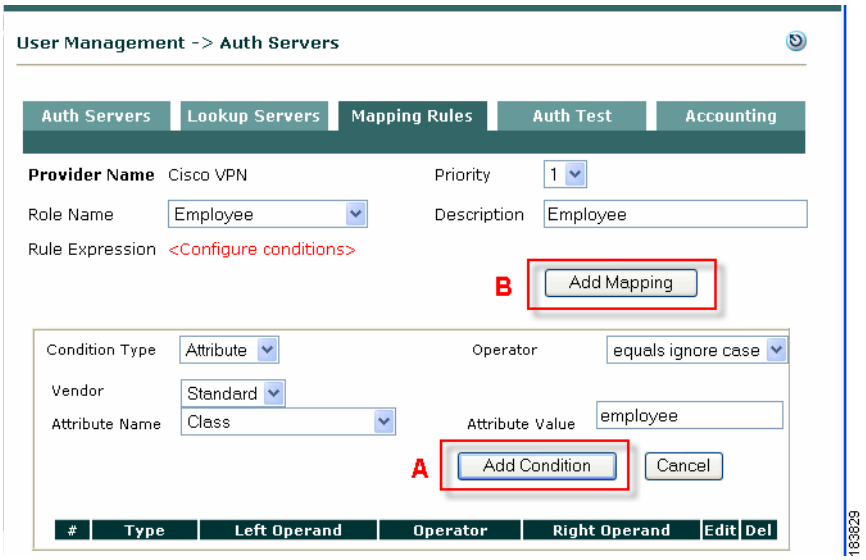


Figure 7-24 Mapping for Cisco VPN Auth Type



2. The **Add Mapping Rule** form appears.

Figure 7-25 Example Add Mapping Rule (Cisco VPN)



Configure Conditions for Mapping Rule (A)

- **Provider Name**—The Provider Name sets the fields of the Mapping Rules form for that authentication server type. For example, the form only allows VLAN ID mapping rule configuration for Kerberos, Windows NT, Windows NetBIOS SSO, and S/Ident auth server types. The form allows VLAN ID or Attribute mapping rule configuration for RADIUS, LDAP, and Cisco VPN SSO auth types.
- **Condition Type**—Configure and add conditions first (step **A** in Figure 7-25) before adding the mapping rule. Choose one of the following from the dropdown menu to set the fields of the Condition form:
  - **Attribute**—For LDAP, RADIUS, Cisco VPN SSO auth providers only.
  - **VLAN ID**—All auth server types.
  - **Compound**—This condition type only appears after you have at least one condition statement already added to the mapping rule (see Figure 7-29 on page 7-37). It allows you to combine individual conditions using boolean operators. You can combine VLAN ID conditions with operators: equals, not equals, belongs to. You can combine Attribute conditions alone, or mixed VLAN ID and Attribute conditions with operators: AND, OR, or NOT. For compound

conditions, instead of associating attribute types to attribute values, you choose two existing conditions to associate together, which become Left and Right Operands for the compound statement.

3. **Attribute Name**—Depending on the context, this field appears as follows:
   - For a **VLAN ID** condition type (Figure 7-26), this field is called **Property Name** and is populated by default with "VLAN ID" (and disabled for editing).
   - For LDAP servers (Figure 7-27), **Attribute Name** is a text field into which you type the source attribute you want to test. The name must be identical (case-sensitive) to the name of the attribute passed by the authentication source, unless you choose the **equals ignore case** operator to create the condition.

     Note You cannot reliably use the "memberOf" attribute to determine the user's Primary Group in an LDAP Active Directory Group membership query. Therefore, you must use a workaround method to be able to map the user's Primary Group VLAN ID, based on Active Directory group membership.

     For more information, see the following Microsoft Knowledge Base articles:
     http://support.microsoft.com/kb/275523
     http://support.microsoft.com/kb/321360

   - For Cisco VPN servers, **Attribute Name** is a dropdown menu (Figure 7-30) with the following options: Class, Framed_IP_Address, NAS_IP_Address, NAS_Port, NAS_Port_Type, User_Name, Tunnel_Client_Endpoint, Service_Type, Framed_Protocol, Acct_Authentic
4. For RADIUS servers (Figure 7-28), the Condition fields are populated differently:
   - **Vendor**—Choose Standard, Cisco, Microsoft, or WISPr (Wireless Internet Service Provider roaming) from the dropdown menu.
   - **Attribute Name**—Choose from the set of attributes for each **Vendor** from the dropdown menu. For example, Standard has 253 attributes (Figure 7-31), Cisco has 30 attributes (Figure 7-32), Microsoft has 32 attributes (Figure 7-33), and WISPr has 11 attributes (Figure 7-33).

     Note For RADIUS servers, only attributes returned in the "access-accept" packet are used for mapping.

   - **Data Type**—(Optional) You can optionally specify Integer or String according to the value passed by the **Attribute Name.** If no data type is specified, **Default** is used.
5. **Attribute Value**—Type the value to be tested against the source **Attribute Name**.
6. **Operator (Attribute)**—Choose the operator that defines the test of the source attribute string.
   - **equals** – True if the value of the **Attribute Name** matches the **Attribute Value**.
   - **not equals** – True if the value of the **Attribute Name** does not match the **Attribute Value**.
   - **contains**– True if the value of the **Attribute Name** contains the **Attribute Value**.
   - **starts with** – True if the value of the **Attribute Name** begins with the **Attribute Value**.
   - **ends with** – True if the value of the **Attribute Name** ends with the **Attribute Value**.
   - **equals ignore case** – True if the value of the **Attribute Name** matches the **Attribute Value** string, regardless of whether the string is uppercase or lowercase.

7. **Operator (VLAN ID)**—If you choose VLAN ID as the **Condition Type**, choose one of the following operators to define a condition that tests against VLAN ID integers.
   - **equals** – True if the VLAN ID matches the VLAN ID in the **Property Value** field.
   - **not equals** – True if the VLAN ID does not match the VLAN ID in the **Property Value** field.
   - **belongs to** – True if the VLAN ID falls within the range of values configured for the **Property Value** field. The value should be one or more comma separated VLAN IDs. Ranges of VLAN IDs can be specified by hyphen (-), for example, [2,5,7,100-128,556-520]. Only integers can be entered, not strings. Note that brackets are optional.

Note For the Cisco VPN SSO type, VLAN IDs may not be available for mapping if there are multiple hops between the CAS and the VPN concentrator.

8. **Add Condition (Save Condition)**—Make sure to configure the condition, then click **Add Condition** to add the condition to the rule expression (otherwise your configuration is not saved).

Add Mapping Rule to Role (B)

Add the mapping rule (step **B** in Figure 7-25) after you have configured and added the condition(s).

9. **Role Name**—After you have added at least one condition, choose the user role to which you will apply the mapping from the dropdown menu.
10. **Priority**—Select a priority from the dropdown to determine the order in which mapping rules are tested. The first rule that evaluates to true is used to assign the user a role.
11. **Rule Expression**—To aid in configuring conditional statements for the mapping rule, this field displays the contents of the last Condition to be added. After adding the condition(s), you must click **Add Mapping Rule** to save all the conditions to the rule.
12. **Description**—An optional description of the mapping rule.
13. **Add Mapping (Save Mapping)**—Click this button when done adding conditions to create the mapping rule for the role. You have to Add or Save the mapping for a specified role, or your configuration and your conditions will not be saved.

Figure 7-26 Example Add VLAN ID Mapping Rule

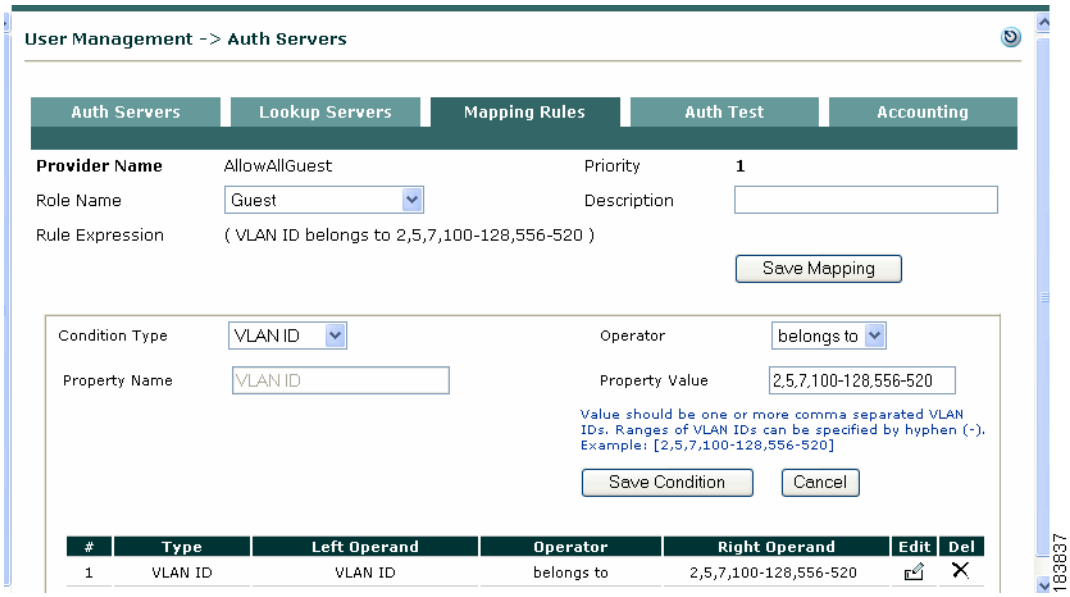


Figure 7-27 Example Add LDAP Mapping Rule (Attribute)

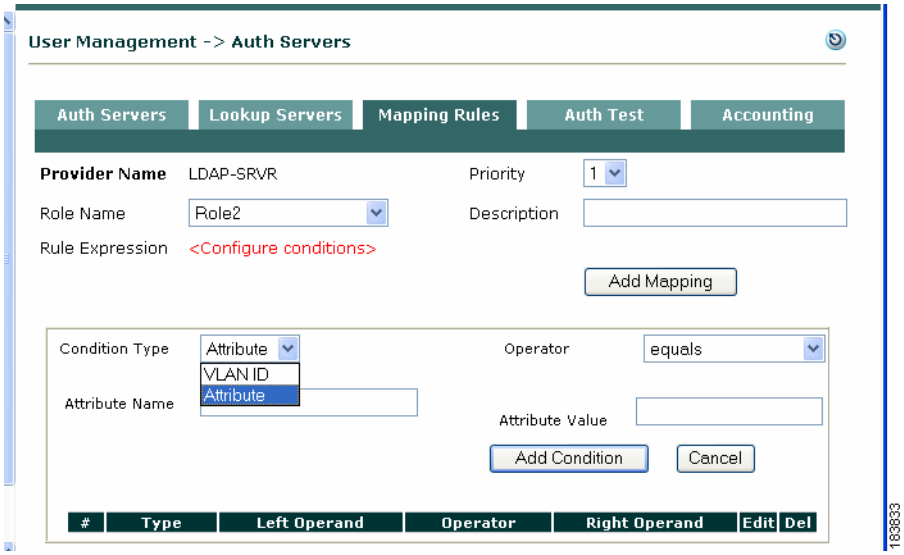


Figure 7-28 Example Add RADIUS Mapping Rule (Attribute)

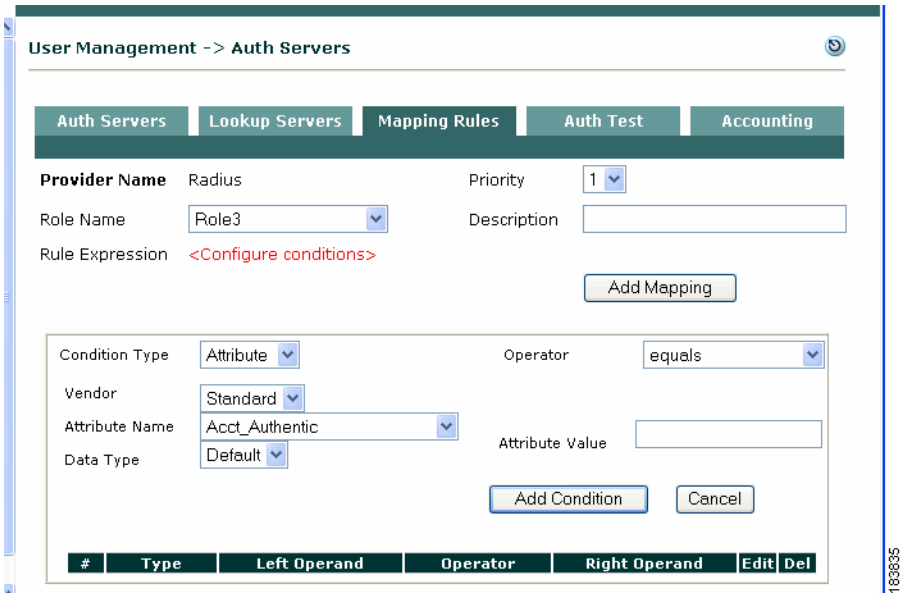
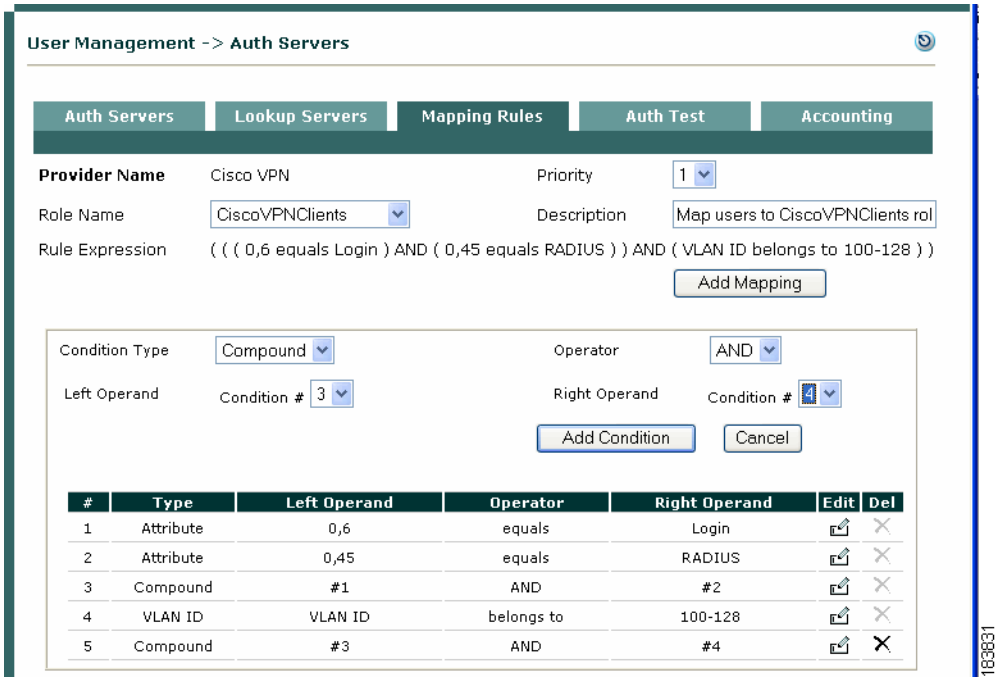


Figure 7-29 Example Compound Condition Mapping Rules



Editing Mapping Rules

Priority—To change the priority of a mapping rule later, click the up/down arrow next to the entry in the **User Management > Auth Servers > List**. The priority determines the order in which the rules are tested. The first rule that evaluates to true is used to assign the user to a role.

Edit—Click the Edit icon next to the rule to modify the mapping rule, or delete conditions from the rule. Note that when editing a compound condition, the conditions below it (created later) are not displayed. This is to avoid loops.

Delete—Click the delete icon next to the Mapping Rule entry for an auth server to delete that individual mapping rule. Click the delete icon next to a condition on the Edit mapping rule form to remove that condition from the Mapping Rule. Note that you cannot remove a condition that is dependent on another rule in a compound statement. To delete an individual condition, you have to delete the compound condition first.

Figure 7-30 CiscoVPN—Standard Attribute Names

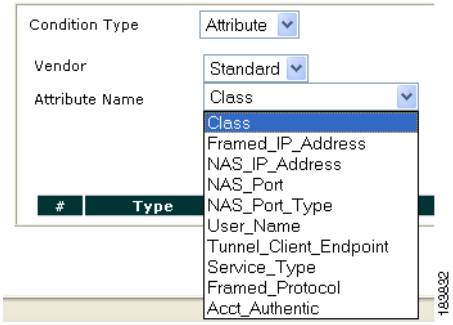


Figure 7-31 RADIUS—Standard Attribute Names

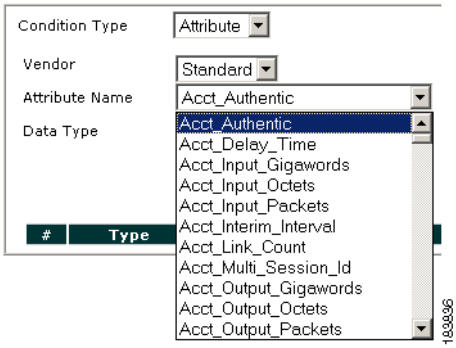


Figure 7-32 RADIUS—Cisco Attribute Names

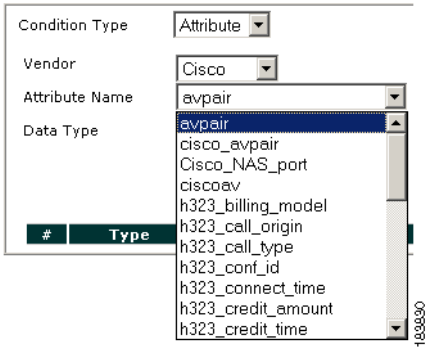


Figure 7-33 RADIUS—Microsoft Attribute Names

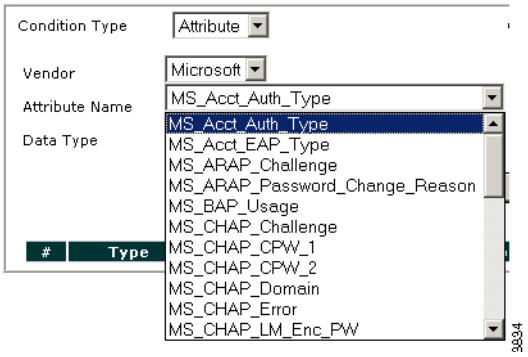
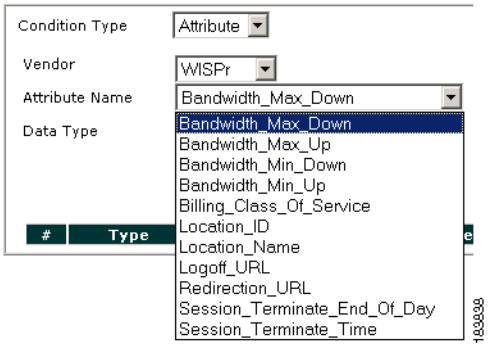


Figure 7-34 RADIUS—WISPr (Wireless Internet Service Provider roaming) Attribute Names



Auth Test

The **Auth Test** tab is allows you to test Kerberos, RADIUS, Windows NT, LDAP, and AD SSO authentication providers you configured against actual user credentials, and lists the role assigned to the user. Error messages are provided to assist in debugging authentication sources, particularly LDAP and RADIUS servers.

To use the **Auth Test** function to test AD SSO authentication in Cisco NAC Appliance, you must perform the following set-up steps, as described in the "Configuring Active Directory Single Sign-On (AD SSO)" chapter of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*, before testing AD SSO server authentication:

1. Create an LDAP Lookup Server as described in the "Add LDAP Lookup Server for Active Directory SSO (Optional)" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.
2. Create an AD SSO authentication provider and associate the AD SSO authentication provider with the LDAP Lookup Server using the **LDAP Lookup Server** field, as described in the "Add Active Directory SSO Auth Server" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Tip When creating or making changes to an existing authentication provider, create a new Auth Server entry that points to the staging or development setup. You can then use **Auth Test** to test the setup prior to production deployment.

Note You cannot use Auth Test to test SSO. A client machine is needed to test SSO.

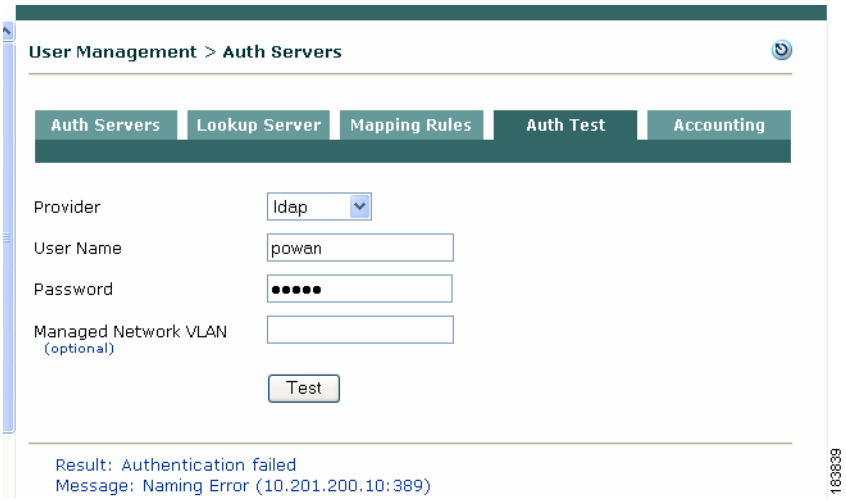
To test authentication:

Step 1 From **User Management > Auth Servers > Auth Test** tab, select the provider against which you want to test credentials in the **Provider** list. If the provider does not appear, make sure it is correctly configured in the **List** tab.

Step 2 Type the username and password (if required) for the user, and the appropriate VLAN ID value if needed.

Step 3 Click **Submit**. The test results appear at the bottom of the page.

Figure 7-35 Auth Test



Authentication Successful

For any provider type, the **Result** "Authentication successful" and **Role** of the user are displayed when the auth test succeeds.

For LDAP/RADIUS servers, when authentication is successful and mapping rules are configured, the attributes/values specified in the mapping rule are also displayed if the auth server (LDAP/RADIUS) returns those values. For example:

```
Result: Authentication successful
Role: <role name>
Attributes for Mapping:
    <Attribute Name>=<Attribute value>
```

Authentication Failed

When authentication fails, a **Message** displays along with the "Authentication failed" result. Table 7-1 illustrates some example authentication test failure messages.

Table 7-1 Example "Authentication Failed" Results

Message	Description
`Message: Invalid User Credential`	Correct user name, incorrect password
`Message: Unable to find the full DN for user <User Name>`	Correct password, incorrect user name (LDAP provider)
`Message: Client Receive Exception: Packet Receive Failed (Receive timed out)`	Correct password, incorrect user name (RADIUS provider)
`Message: Invalid Admin(Search) Credential`	Correct user name, correct password, incorrect value configured in the **Search(Admin) Full DN** field of the Auth provider (e.g. incorrect CN configured for LDAP Server)
`Message: Naming Error (x.x.x.x: x)`	Correct user name, correct password, incorrect value configured in the **Server URL** field of the Auth provider (e.g. incorrect port or URL configured for LDAP)

Note The **Auth Test** feature does not apply to S/Ident, Windows NetBIOS SSO, and Cisco VPN SSO authentication provider types.

RADIUS Accounting

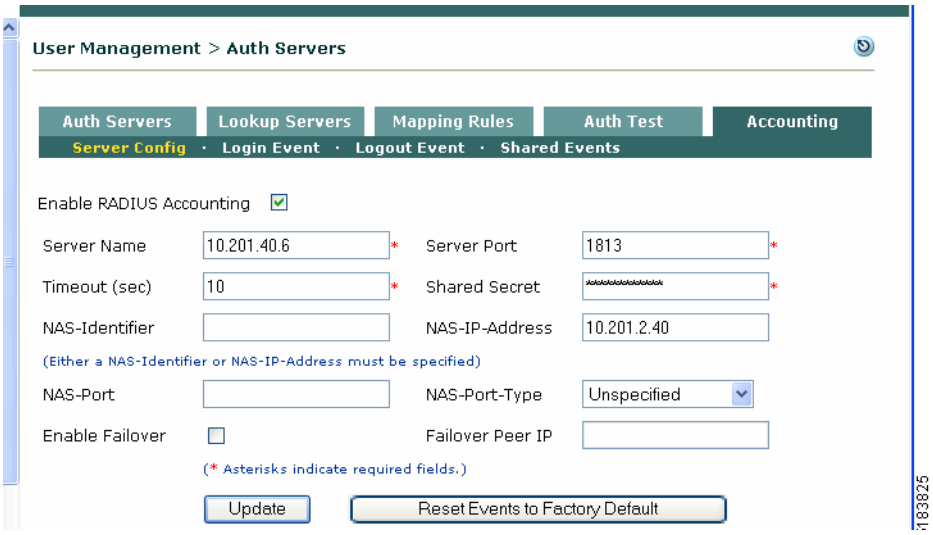
The Clean Access Manager can be configured to send accounting messages to a RADIUS accounting server. The CAM sends a **Start** accounting message when a user logs into the network and sends a **Stop** accounting message when the user logs out of the system (or is logged out or timed out). This allows for the accounting of user time and other attributes on the network.

You can also customize the data to be sent in accounting packets for login events, logout events, or shared events (login and logout events).

Enable RADIUS Accounting

Step 1 Go to **User Management > Auth Servers > Accounting > Server Config**.

Figure 7-36 RADIUS Accounting Server Config Page



Step 2 Select **Enable RADIUS Accounting** to enable the Clean Access Manager to send accounting information to the named RADIUS accounting server.

Step 3 Enter values for the following form fields:

- **Server Name**—The fully qualified host name (e.g. auth.cisco.com) or IP address of the RADIUS accounting server.
- **Server Port**—The port number on which the RADIUS server is listening. The Server Name and Server Port are used to direct accounting traffic to the accounting server.
- **Timeout(sec)**—Specifies how long to attempt to retransmit a failed packet.
- **Shared Secret**—The shared secret used to authenticate the Clean Access Manager accounting client with the specified RADIUS accounting server.
- **NAS-Identifier**—The NAS-Identifier value to be sent with all RADIUS accounting packets. Either a NAS-Identifier or a NAS-IP-Address must be specified to send the packets.
- **NAS-IP-Address**—The NAS-IP-Address value to be sent with all RADIUS accounting packets. Either a NAS-IP-Address or a NAS-Identifier must be specified to send the packets.

Note If your CAM is deployed as a member of an HA failover pair, be sure you specify the service IP address for the HA pair to ensure the RADIUS accounting server receives the proper RADIUS accounting packets from the CAM. Regardless of whether the HA-Primary or HA-Standby CAM sends the accounting packets it will show up in the accounting packets as the pair. You must also configure the RADIUS accounting server to accept accounting packets from both the HA-Primary and HA-Secondary CAM eth0 IP addresses to ensure that the RADIUS server accepts the packets regardless of which CAM in the HA pair sends them. This is done in Cisco Secure ACS under AAA Clients.

- **NAS-Port**—The NAS-Port value to be sent with all RADIUS accounting packets.
- **NAS-Port-Type**—The NAS-Port-Type value to be sent with all RADIUS accounting packets.
- **Enable Failover**—This enables sending a second accounting packet to a RADIUS failover peer IP if the primary RADIUS accounting server's response times out.
- **Failover Peer IP**—The IP address of the failover RADIUS accounting server.

Step 4 Click **Update** to update the server configuration.

Restore Factory Default Settings

The Clean Access Manager can be restored to the factory default accounting configuration as follows:

1. Go to **Administration > Backup** to backup your database before restoring default settings.
2. Go to **User Management > Auth Servers > Accounting > Server Config**
3. Click the **Reset Events to Factory Default** button to remove the user configuration and replace it with the Clean Access Manager default accounting configuration.
4. Click OK in the confirmation dialog that appears.

Add Data to Login, Logout or Shared Events

For greater control over the data that is sent in accounting packets, you can add or customize the RADIUS accounting data that is sent for login events, logout events, or shared events (data sent for both login and logout events).

Data Fields

The following data fields apply to all events (login, logout, shared):

- Current Time (Unix Seconds)—The time the event occurred
- Login Time (Unix Seconds)—The time the user logged on.
- CA Manager IP—IP address of the Clean Access Manager
- Current Time (DTF)—Current time in date time format (DTF)
- OS Name—Operating system of the user
- Vlan ID—VLAN ID with which the user session was created.
- User Role Description—Description of the user role of the user
- User Role Name—Name of the user role of the user
- User Role ID—Role ID that uniquely identifies the user role.
- CA Server IP— IP of the Clean Access Server the user logged into.
- CA Server Description—Description of the Clean Access Server the user logged into.
- CA Server Key—Key of the Clean Access Server.
- Provider Name—Authentication provider of the user
- Login Time (DTF)—Login time of the user in date time format (DTF)
- User MAC—MAC address of the user
- User IP—IP address of the user
- User Key—Key with which the user logged in.

Note For Out-of-Band users only, user_key= IP address.

- User Name—User account name.

Logout Event Data Fields

The following four data fields apply to logout events only and are not sent for login or shared events:

- Logout Time (Unix Seconds)—Logout time of the user in Unix seconds.
- Logout Time (DTF)—Logout time of the user in date time format.
- Session Duration (Seconds)—Duration of the session in seconds.
- Termination Reason—Output of the Acct_Terminate_Cause RADIUS attribute.

Add New Entry (Login Event, Logout Event, Shared Event)

To add new data to a RADIUS attribute for a shared event:

The following steps describe how to configure a RADIUS attribute with customized data. The steps below describe a shared event. The same process applies for login and logout events.

1. Go to **User Management > Auth Servers > Accounting**.
2. Click the **Shared Event** (or **Login Event**, **Logout Event**) link to bring up the appropriate page.
3. Click the **New Entry** link at the right-hand side of the page to bring up the add form.

Figure 7-37 New Shared Event

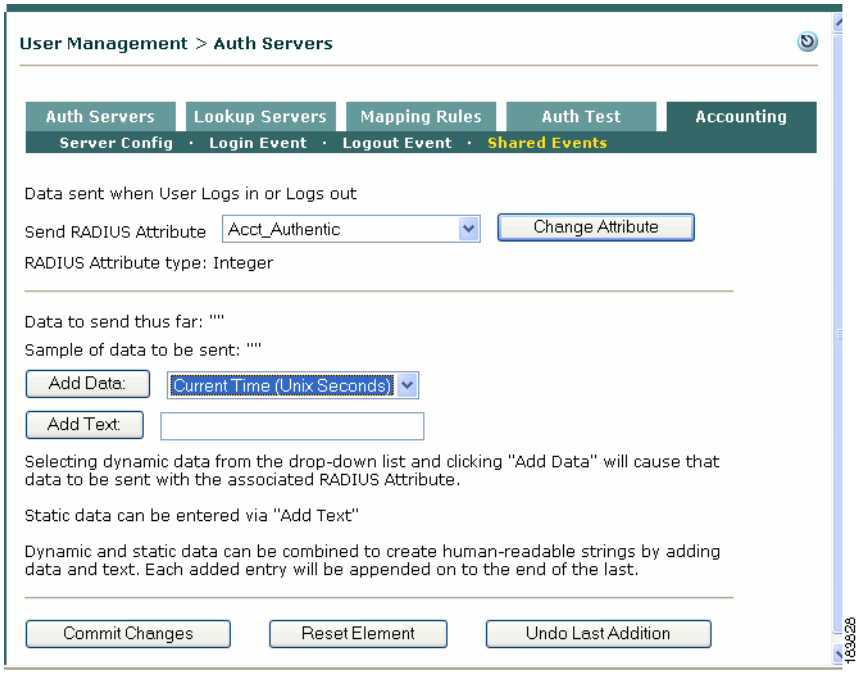
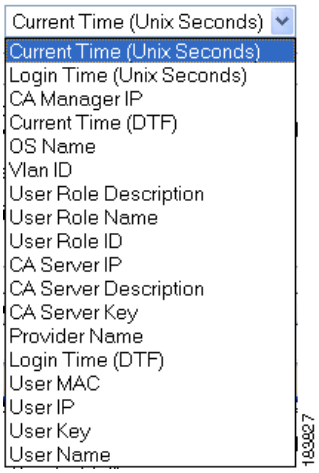

User Management > Auth Servers
Auth Servers
Lookup Servers
Mapping Rules
Auth Test
Accounting
Server Config · Login Event · Logout Event · Shared Events
Data sent when User Logs in or Logs out
Send RADIUS Attribute
Acct_Authentic
Change Attribute
RADIUS Attribute type: Integer
Data to send thus far: ""
Sample of data to be sent: ""
Add Data:
Current Time (Unix Seconds)
Add Text:
Selecting dynamic data from the drop-down list and clicking "Add Data" will cause that data to be sent with the associated RADIUS Attribute.
Static data can be entered via "Add Text"
Dynamic and static data can be combined to create human-readable strings by adding data and text. Each added entry will be appended on to the end of the last.
Commit Changes
Reset Element
Undo Last Addition
169828

Figure 7-38 RADIUS Attribute Dropdown Menu



4. From the **Send RADIUS Attribute** dropdown menu, choose a RADIUS attribute.
5. Click the **Change Attribute** button to update the **RADIUS Attribute type**. The type, such as "String" or "Integer," will display in this field.
6. Configure the type of data to send with the attribute. There are three options:
   - Send static data—In this case, type the text to be added in the **Add Text** text box and click the **Add Text** button. Every time a user logs in/logs out, the RADIUS attribute selected will be sent with the static data entered.
   - Send dynamic data—In this case, select one of the 18 dynamic data variables (or 22 for logout events) from the dropdown menu and click the **Add Data** button. Every time a user logs in/logs out, the dynamic data selected will be replaced with the appropriate value when sent.
   - Send static and dynamic data—In this case, a combination of static and dynamic data is sent. For example:

     User: [User Name] logged in at: [Login Time DTF] from CA Server [CA Server Description]

   See also Figure 7-39, Figure 7-40, and Figure 7-41 show examples of Login, Logout, and Shared events, respectively. for additional details.
7. As data is added, the **Data to send thus far**: field displays all the data types selected to be sent with the attribute, and the **Sample of data to be sent:** field illustrates how the data will appear.
8. Click **Commit Changes** to save your changes.
9. Click the **Reset Element** button to reset the form.
10. Click **Undo Last Addition** to remove the last entry added to the **Data to send thus far**: field.

Figure 7-39, Figure 7-40, and Figure 7-41 show examples of Login, Logout, and Shared events, respectively.

Figure 7-39 Login Events

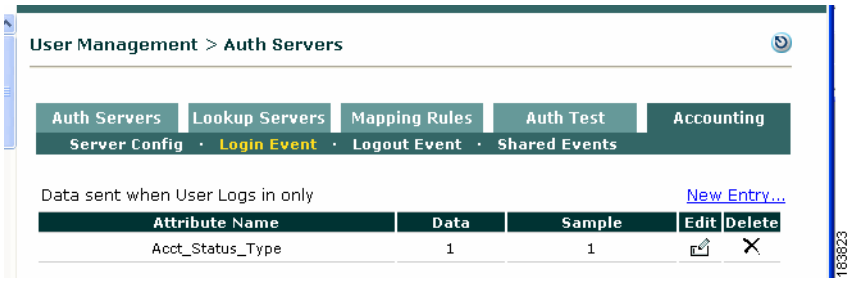


Figure 7-40 Logout Events

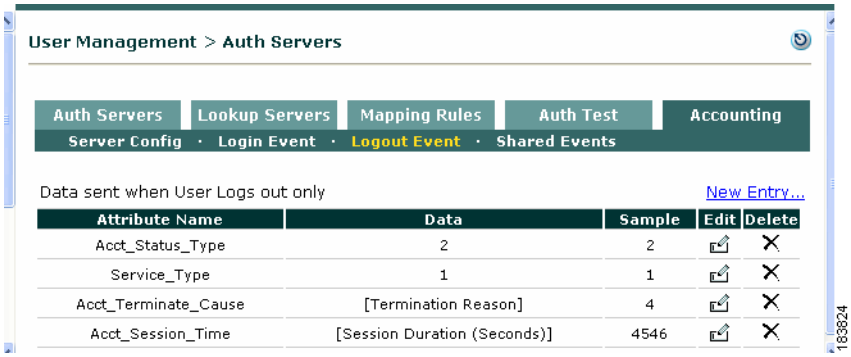
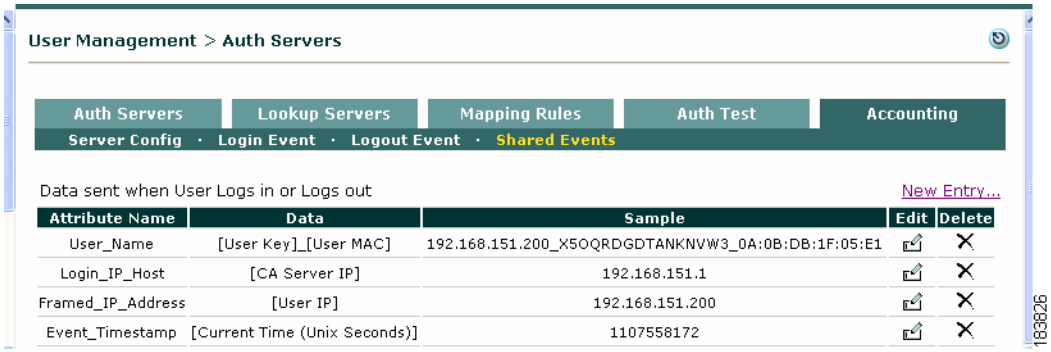


Figure 7-41 Shared Events





User Management: Traffic Control, Bandwidth, Schedule

This chapter describes how to configure role-based traffic control policies, bandwidth management, session and heartbeat timers. Topics include:

- Overview, page 8-1
- Add Global IP-Based Traffic Policies, page 8-4
- Add Global Host-Based Traffic Policies, page 8-8
- Control Bandwidth Usage, page 8-13
- Configure User Session and Heartbeat Timeouts, page 8-15
- Configure Policies for Agent Temporary and Quarantine Roles, page 8-19
- Example Traffic Policies, page 8-24
- Troubleshooting Host-Based Policies, page 8-29

For details on configuring user roles and local users, see Chapter 6, "User Management: Configuring User Roles and Local Users."

For details on configuring authentication servers, see Chapter 7, "User Management: Configuring Authentication Servers."

For details on creating and configuring the web user login page, see Chapter 5, "Configuring User Login Page and Guest Access."

Overview

You can control the In-Band user traffic that flows through the Clean Access Server with a variety of mechanisms. This section describes the Traffic Control, Bandwidth, and Scheduling policies configured by user role.

For new deployments of Cisco NAC Appliance, by default all traffic from the trusted to the untrusted network is allowed, and traffic from the untrusted network to the trusted network is blocked for the default system roles (Unauthenticated, Temporary, Quarantine) and new user roles you create. This allows you to expand access as necessary for traffic sourced from the untrusted network.

Cisco NAC Appliance offers three types of traffic policies:

IP-based policies—IP-based policies are fine-grained and flexible and can stop traffic in any number of ways. IP-based policies are intended for any role and allow you to specify IP protocol numbers as well as source and destination port numbers. For example, you can create an IP-based policy to pass through IPSec traffic to a particular host while denying all other traffic.

Host-based policies—Host-based policies are less flexible than IP-based policies, but have the advantage of allowing traffic policies to be specified by host name or domain name when a host has multiple or dynamic IP addresses. Host-based policies are intended to facilitate traffic policy configuration primarily for Agent Temporary and Quarantine roles and should be used for cases where the IP address for a host is continuously changing or if a host name can resolve to multiple IPs.

Layer 2 Ethernet traffic policies—To support data transfer or similar operations originating at the Layer 2 level, Cisco NAC Appliance Layer 2 Ethernet traffic control policies enable you to allow or deny Layer 2 Ethernet traffic through the CAS based on the type of traffic. Network Frames except for IP, ARP, and RARP frames constitute standard Layer 2 traffic.



Note Layer 2 Ethernet traffic control only applies to Clean Access Servers operating in Virtual Gateway mode.

Traffic control policies are directional. IP-based and Layer 2 Ethernet traffic policies can allow or block traffic moving from the untrusted (managed) to the trusted network, or from the trusted to the untrusted network. Host-based policies allow traffic from the untrusted network to the specified host and trusted DNS server specified.

By default, when you create a new user role:

- All traffic from the untrusted network to the trusted network is blocked.
- All traffic from the trusted network to the untrusted network is allowed.

You must create policies to allow traffic as appropriate for the role. Alternatively, you can configure traffic control policies to block traffic to a particular machine or limit users to particular activities, such as email use or web browsing. Examples of traffic policies are:

`deny access to the computer at 191.111.11.1`, or
`allow www communication from computers on subnet 191.111.5/24`

Traffic Policy Priority

Finally, the order of the traffic policy in the policy list affects how traffic is filtered. The first policy at the top of the list has the highest priority. The following examples illustrate how priorities work for Untrusted->Trusted traffic control policies.

Example 1:

1. Deny Telnet
2. Allow All

Result: Only Telnet traffic is blocked and all other traffic is permitted.

Example 2 (priorities reversed):

1. Allow All
2. Deny Telnet

Result: All traffic is allowed, and the second policy blocking Telnet traffic is ignored.

Example 3:

1. Allow TCP *.* 10.10.10.1/255.255.255.255
2. Block TCP *.* 10.10.10.0/255.255.255.0

Result: Allow TCP access to 10.10.10.1 while blocking TCP access to everything else in the subnet (10.10.10.*).

Example 4 (Layer 2 Ethernet - Virtual Gateway mode only):

1. Allow SNA IBM Systems Network Architecture
2. Block ALL All Traffic

Result: Allow only IBM Systems Network Architecture (SNA) Layer 2 traffic and deny all other Layer 2 traffic.

Global vs. Local Scope

This chapter describes global traffic control policies configured under **User Management > User Roles > Traffic Control**. For details on local traffic control policies configured under **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Note A local traffic control policy in a specific CAS takes precedence over a global policy if the local policy has a higher priority.

Traffic policies you add using the global forms under **User Management > User Roles > Traffic Control** apply to all Clean Access Servers in the CAM's domain and appear with white background in the global pages.

Global traffic policies are displayed for a local CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles** and appear with yellow background in the local list.

To delete a traffic control policy, use the global or local form you used to create it.

Pre-configured default host-based policies apply globally to all Clean Access Servers and appear with yellow background in both global and local host-based policy lists. These default policies can be enabled or disabled, but cannot be deleted. See Enable Default Allowed Hosts, page 8-9 for details.

View Global Traffic Control Policies

Click the **IP** subtab link to configure IP-based traffic policies under **User Management > User Roles > Traffic Control > IP** (Figure 8-2).

Click the **Host** subtab link to configure Host-based traffic policies under **User Management > User Roles > Traffic Control > Host**. (Figure 8-7).

Click the **Ethernet** subtab link to configure Layer 2 Ethernet traffic control policies under **User Management > User Roles > Traffic Control > Ethernet**. (Figure 8-9)

By default, IP-based traffic policies for roles are shown with the untrusted network as the source and the trusted network as the destination of the traffic. To configure policies for traffic traveling in the opposite direction, choose **Trusted->Untrusted** from the source-to-destination direction field and click **Select**.

You can view IP, Host-based, or Layer 2 Ethernet traffic policies for "All Roles" or a specific role by choosing from the role dropdown menu and clicking the **Select** button (Figure 8-1).

Figure 8-1 Trusted -> Untrusted Direction Field



Add Global IP-Based Traffic Policies

You can configure traffic policies for all the default roles already present in the system (Unauthenticated, Temporary, Quarantine). You will need to create normal login user roles first before you can configure traffic policies for them (see Chapter 6, "User Management: Configuring User Roles and Local Users.")

This section describes the following:

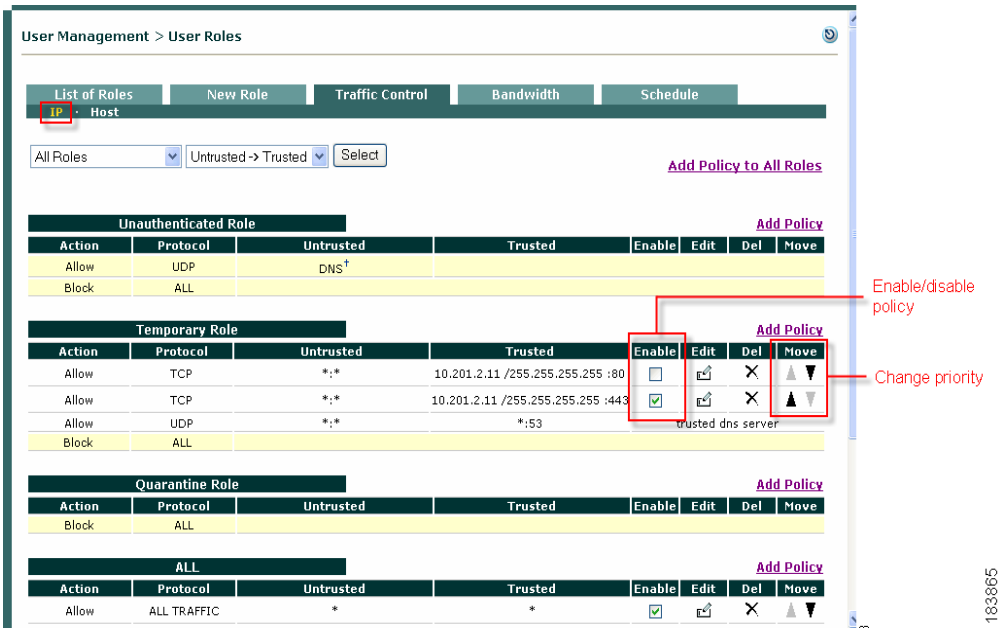
- Add IP-Based Policy, page 8-4
- Edit IP-Based Policy, page 8-7

Add IP-Based Policy

You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring IP-based traffic policies.

1. Go to **User Management > User Roles > Traffic Control > IP**. The list of IP-based policies for all roles displays (Figure 8-2).

Figure 8-2 List of IP-Based Policies



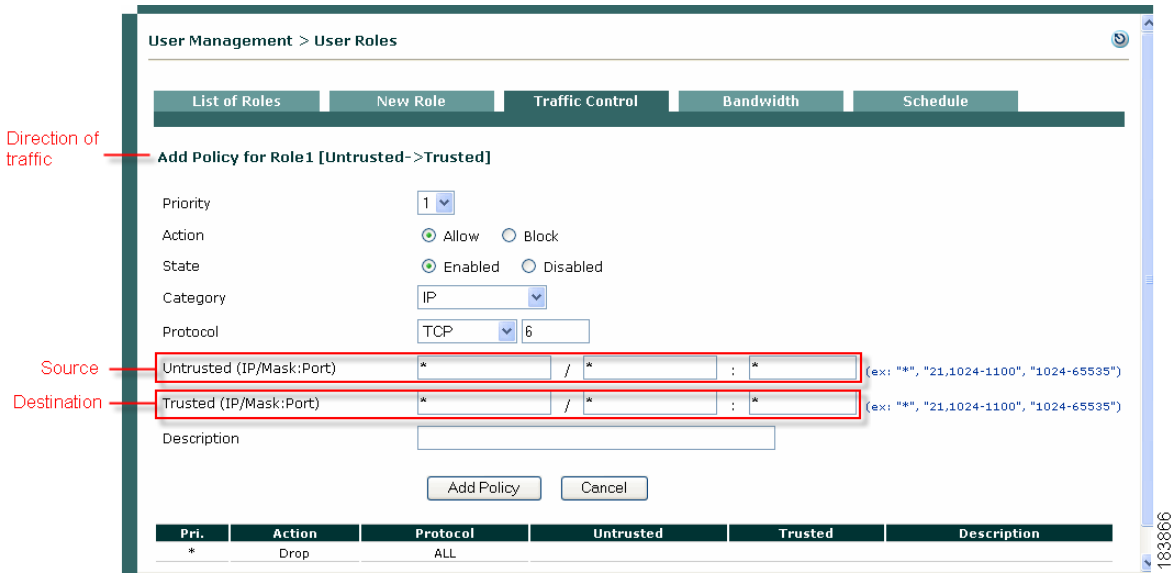
2. Select the source-to-destination direction for which you want the policy to apply. Chose either **Trusted->Untrusted** or **Untrusted->Trusted**, and click **Select**.

3. Click the **Add Policy** link next to the user role to create a new policy for the role, or click **Add Policy to All Roles** to add the new policy to all roles (except the Unauthenticated role) at once.

Note The **Add Policy to All Roles** option adds the policy to all roles except the Unauthenticated role. Once added, traffic policies are modified individually and removed per role only.

4. The **Add Policy** form for the role appears (Figure 8-3).

Figure 8-3 Add IP-Based Policy



5. Set the **Priority** of the policy from the **Priority** dropdown menu. The IP policy at the top of the list will have the highest priority in execution. By default, the form displays a priority lower than the last policy created (1 for the first policy, 2 for the second policy, and so on). The number of priorities in the list reflects the number of policies created for the role. The built-in **Block All** policy has the lowest priority of all policies by default.

Note To change the **Priority** of a policy later, click the Up or Down arrows for the policy in the **Move** column of the IP policies list page (Figure 8-2).

6. Set the **Action** of the traffic policy as follows:
   - **Allow** (default)—Permit the traffic.
   - **Block**—Drop the traffic.
7. Set the **State** of the traffic policy as follows:
   - **Enabled** (default)—Enable this traffic policy immediately for any new traffic for the role.
   - **Disabled**—Disable this traffic policy for the role, while preserving the settings of the policy for future use.

Note To enable/disable traffic policies at the role level, click the corresponding checkbox in **Enable** column of the IP policies list page (Figure 8-2).

8. Set the **Category** of the traffic as follows:
   - **ALL TRAFFIC** (default)—The policy applies to all protocols and to all trusted and untrusted source and destination addresses.
   - **IP**—If selected, the **Protocol** field displays as described below.
   - **IP FRAGMENT**—By default, the Clean Access Manager blocks IP fragment packets, since they can be used in denial-of-service (DoS) attacks. To permit fragmented packets, define a role policy allowing them with this option.
9. The **Protocol** field appears if the **IP** Category is chosen, displaying the options listed below:
   - **CUSTOM:**—Select this option to specify a different protocol number than the protocols listed in the **Protocol** dropdown menu.
   - **TCP (6)**—Select for Transmission Control Protocol. TCP applications include HTTP, HTTPS, and Telnet.
   - **UDP (17)**—Select for User Datagram Protocol, generally used for broadcast messages.
   - **ICMP (1)**—Select for Internet Control Message Protocol. If selecting ICMP, also choose a **Type** from the dropdown menu.
   - **ESP (50)**—Select for Encapsulated Security Payload, an IPsec subprotocol used to encrypt IP packet data typically in order to create VPN tunnels.
   - **AH (51)**—Select for Authentication Header, an IPSec subprotocol used to compute a cryptographic checksum to guarantee the authenticity of the IP header and packet.
10. In the **Untrusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the untrusted network to which the policy applies. An asterisk in the IP/Mask:Port fields means the policy applies for any address/application.
    If you chose TCP or UDP as the **Protocol**, also type the TCP/UDP port number for the application in the **Port** text field.

Note You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring TCP/UDP ports. For example, you can specify port values such as: "*****" or "**21, 1024-1100**" or "**1024-65535**" to cover multiple ports in one policy. Refer to http://www.iana.org/assignments/port-numbers for details on TCP/UDP port numbers.

11. In the **Trusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the trusted network to which the policy applies. An asterisk in the IP/Mask:Port fields means the policy applies for any address/application. If you chose TCP or UDP as the **Protocol**, also type the TCP/UDP port number for the application in the **Port** text field.

Note The traffic direction you select for viewing the list of policies (Untrusted -> Trusted or Trusted -> Untrusted) sets the source and destination when you open the **Add Policy** form:

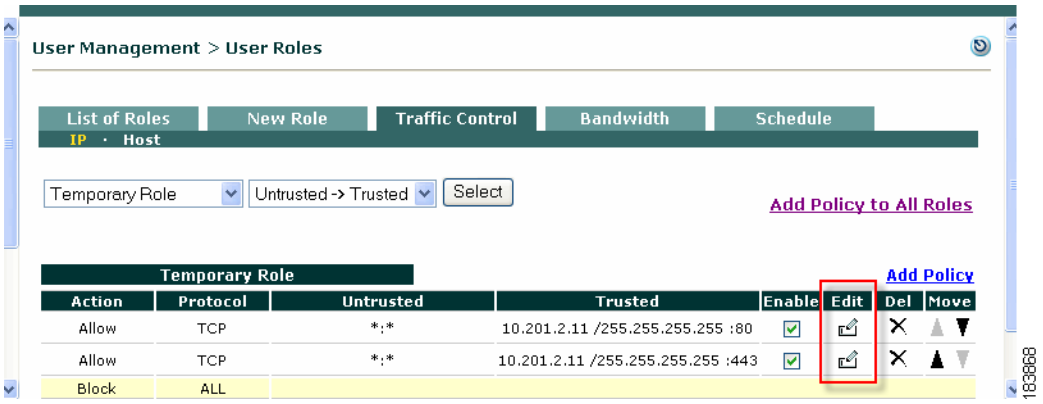
- The first IP/Mask/Port entry listed is the source.
- The second IP/Mask/Port entry listed is the destination.

12. Optionally, type a description of the policy in the **Description** field.
13. Click **Add Policy** when finished. If modifying a policy, click the **Update Policy** button.

Edit IP-Based Policy

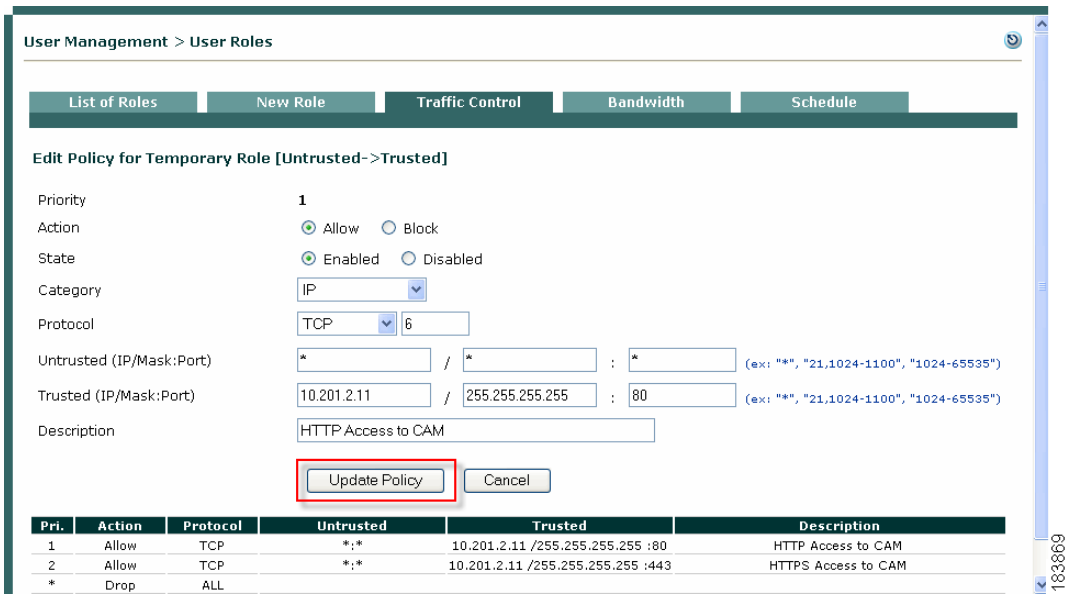
1. Go to **User Management > User Roles > Traffic Control > IP**.
2. Click the **Edit** icon for the role policies you want to edit (Figure 8-4).

Figure 8-4 Edit IP Policy



3. The **Edit Policy** form for the role policy appears (Figure 8-5).

Figure 8-5 Edit IP Policy Form



4. Change properties as desired.

Note You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards such as: "*****" or "**21, 1024-1100**" or "**1024-65535**" for TCP/UDP ports. See http://www.iana.org/assignments/port-numbers for details on TCP/UDP ports.

5. Click **Update Policy** when done.

Note that you cannot change the policy priority directly from the **Edit** form. To change a **Priority**, click the Up or Down arrows for the policy in the **Move** column of the IP policies list page.

Add Global Host-Based Traffic Policies

Default host policies for the Unauthenticated, Temporary, and Quarantine roles are automatically retrieved and updated after an Agent **Update** or **Clean Update** is performed from the CAM (see Retrieving Cisco NAC Appliance Updates, page 9-12 for complete details on Updates).

You can configure custom DNS host-based policies for a role by host name or domain name when a host has multiple or dynamic IP addresses. Once the host-based policy is setup and all the IP Addresses are resolved, it enables all traffic types to the host machine.

Allowing DNS addresses to be configured per user role facilitates client access to the Windows or antivirus update sites that enable clients to fix their systems if Agent requirements are not met or network scanning vulnerabilities are found. Note that to use any host-based policy, you must first add a Trusted DNS Server for the user role.

Note

- After a software upgrade, new default host-based policies are disabled by default but enable/disable settings for existing host-based policies are preserved.
- After a Clean Update, all existing default host-based policies are removed and new default host-based policies are added with default disabled settings.
- The host-based policies have higher priority than IP-based Traffic Policies. The traffic that passes through an allowed host is always allowed, even if an IP-based policy denies it.

This section describes the following:

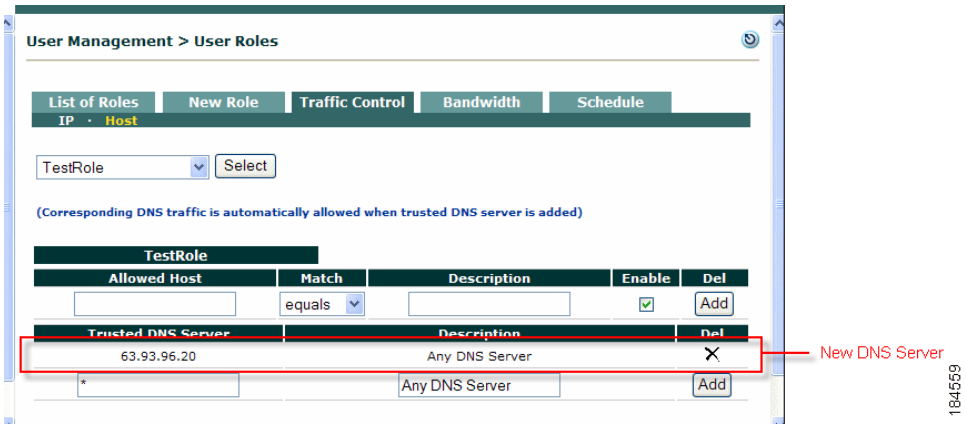
- Add Trusted DNS Server for a Role, page 8-8
- Enable Default Allowed Hosts, page 8-9
- Add Allowed Host, page 8-10
- Proxy Servers and Host Policies, page 8-12

Add Trusted DNS Server for a Role

To enable host-based traffic policies for a role, add a Trusted DNS Server for the role.

1. Go to **User Management > User Roles > Traffic Control** and click the **Host** link.
1. Select the role for which to add a trusted DNS server.
2. Type an IP address in the **Trusted DNS Server** field, or an asterisk "*" to specify any DNS server.

Figure 8-6 Add Trusted DNS Server



3. Optionally type a description for the DNS server in the **Description** field.
4. The **Enable** checkbox should already be selected.
5. Click **Add**. The new policy appears in the **Trusted DNS Server** column.

Note

- When a Trusted DNS Server is added on the **Host** form, an IP-based policy allowing DNS/UDP traffic to that server is automatically added for the role (on the **IP** form).
- When you add a specific DNS server, then later add Any ("*") DNS server to the role, the previously added server becomes a subset of the overall policy allowing all DNS servers, and will not be displayed. If you later delete the Any ("*") DNS server policy, the specific trusted DNS server previously allowed is again displayed.

Enable Default Allowed Hosts

Cisco NAC Appliance provides default host policies for the Unauthenticated, Temporary, and Quarantine roles. Default Host Policies are initially pulled down to your system, then dynamically updated, through performing a Cisco NAC Appliance **Update** or **Clean Update**. Newly added Default Host Policies are disabled by default, and must be enabled for each role under **User Management > User Roles > Traffic Control > Hosts**.

To enable Default Host Policies for user roles:

Step 1 Go to **Device Management > Clean Access > Updates**. (See Figure 9-5 on page 9-15.)

Step 2 Click **Update** to get the latest Default Host Policies (along with Cisco NAC Appliance updates). Updating Default Host Policies does not overwrite any user-defined settings for existing Default Host Policies.

Step 3 Go to **User Management > User Roles > Traffic Control > Host**. (see Figure 8-7 on page 8-10.)

Step 4 Choose the role (Unauthenticated, Temporary, or Quarantine) for which to enable a Default Host Policy from the dropdown menu and click **Select**.

Step 5 Click the **Enable** checkbox for each default host policy you want to permit for the role.

Step 6 Make sure a Trusted DNS server is added (see Add Trusted DNS Server for a Role, page 8-8).

Step 7 To add additional custom hosts for the roles, follow the instructions for Add Allowed Host, page 8-10.

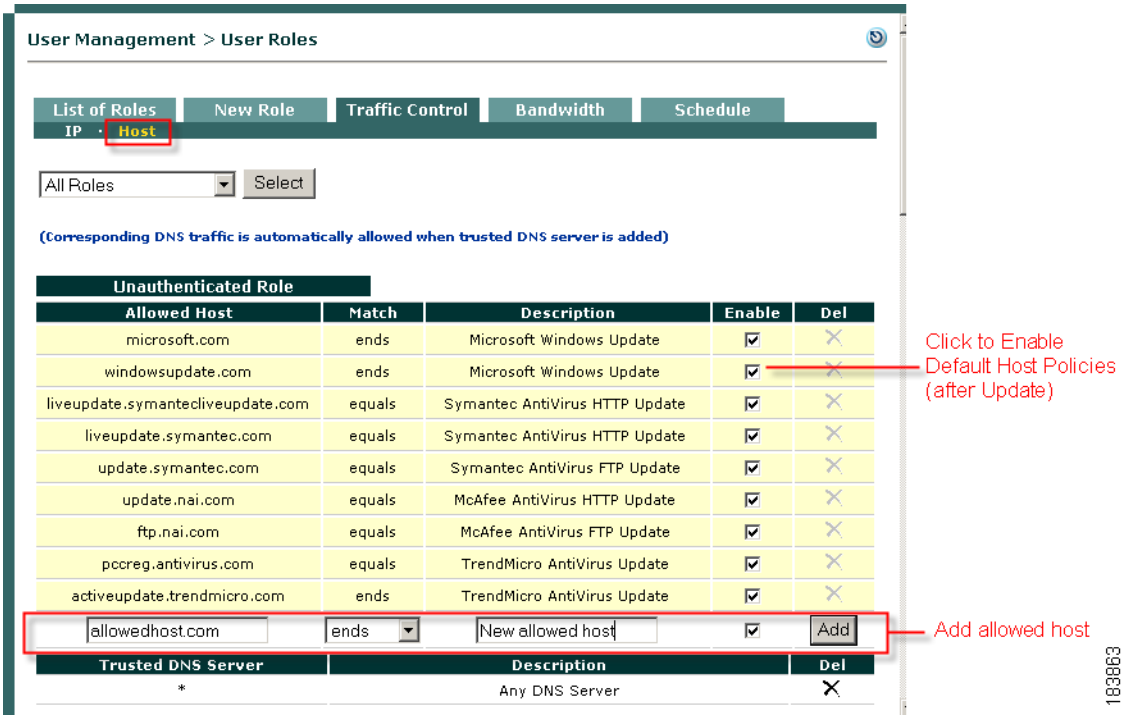
Note See Retrieving Cisco NAC Appliance Updates, page 9-12, for complete details on configuring Updates.

Add Allowed Host

The Allowed Host form allows you to supplement Default Host Policies with additional update sites for the default roles, or create custom host-based traffic policies for any user role.

1. Go to **User Management > User Roles > Traffic Control** and click the **Host** link.

Figure 8-7 Add Allowed Host



2. Select the role for which to add a DNS host.
3. Type the hostname in the **Allowed Host** field (e.g. “allowedhost.com”).
4. In the **Match** dropdown menu, select an operator to match the host name: **equals**, **ends**, **begins**, or **contains**.
5. Type a description for the host in the **Description** field (e.g. “Allowed Update Host”).
6. The **Enable** checkbox should already be selected.
7. Click **Add**. The new policy appears above the **Add** field.

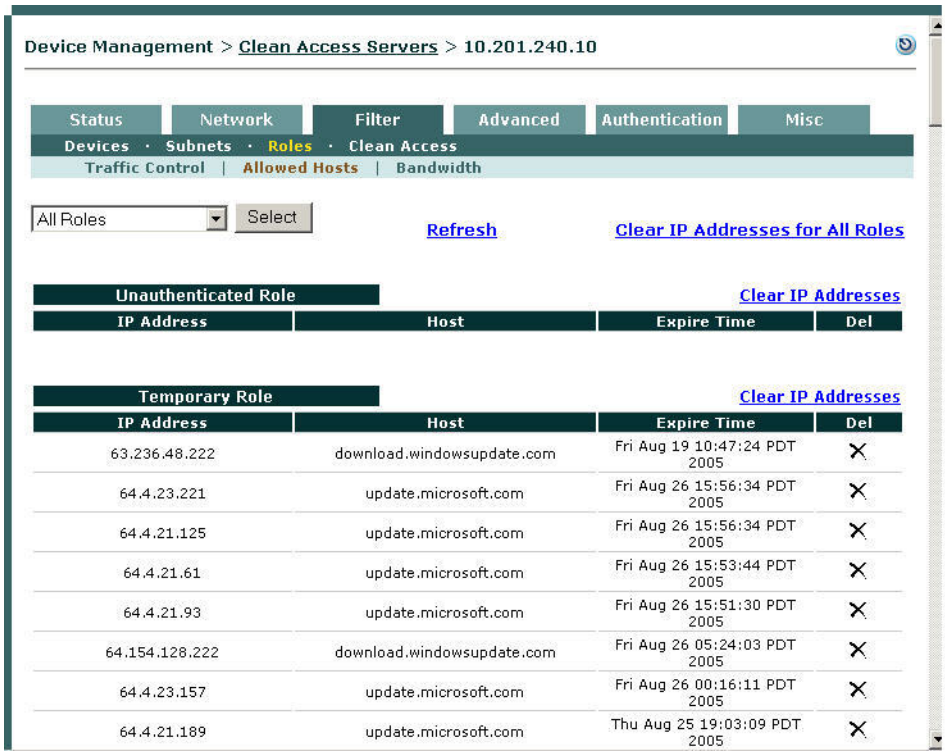
Note You must add a Trusted DNS Server to the role to enable host-based traffic policies for the role.

View IP Addresses Used by DNS Hosts

You can view the IP addresses used for the DNS host when clients connect to the host to update their systems. Note that these IP addresses are viewed per Clean Access Server from the CAS management pages.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts**.
2. To view all IP addresses for DNS hosts accessed across all roles, click the **View Current IP addresses for All Roles** at the top of the page.
3. To view the IP addresses for DNS hosts accessed by clients in a specific role, click the **View Current IP addresses** link next to the desired role.
4. The **IP Address**, **Host Name**, and **Expire Time** will display for each IP address accessed. Note that the Expire Time is based on the DNS reply TTL. When the IP address for the DNS host reaches the Expire Time, it becomes invalid.

Figure 8-8 View Current IP Addresses for All Roles



Tip To troubleshoot host-based policy access, try performing an `ipconfig /flushdns` from a command prompt of the test client machine. Cisco NAC Appliance needs to see DNS responses before putting corresponding IP addresses on the allow list.

Proxy Servers and Host Policies

You can allow users to access only the host sites enabled for a role (e.g. Temporary or Quarantine users that need to meet requirements) when a proxy server specified on the CAS is used.

Note that proxy settings are local policies configured on the CAS using the CAS management pages, and the following pages must be configured to enable this feature:

- **Device Management > Clean Access Servers > Manage [CAS_IP] > Advanced > Proxy**
- **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** (the **Parse Proxy Traffic** option must be enabled)

For complete details, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

See also Proxy Settings, page 5-2 for related information.

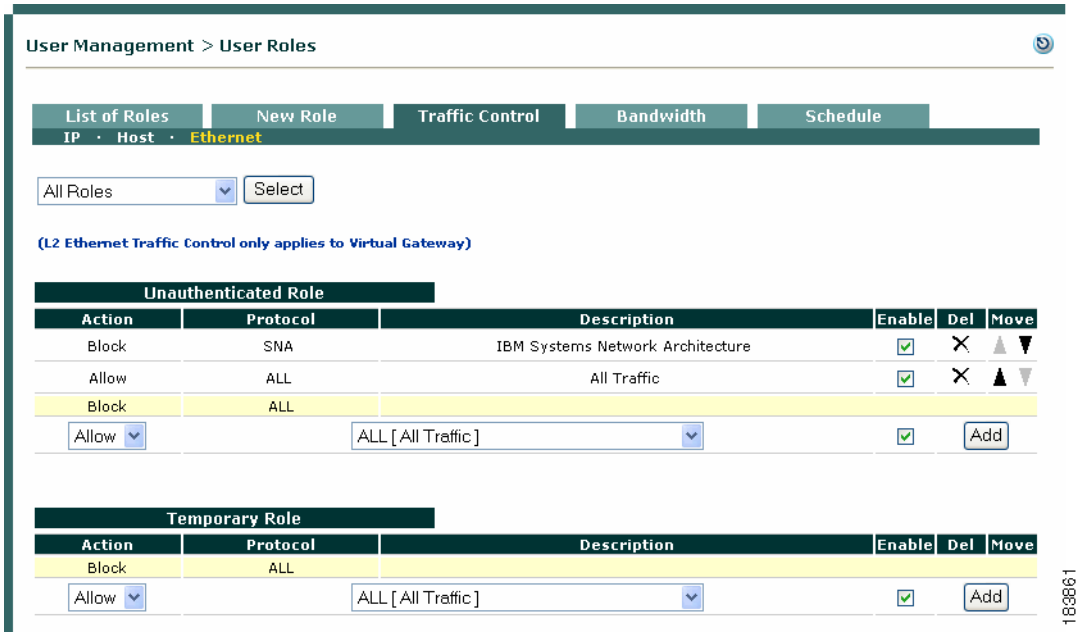
Add Global Layer 2 Ethernet Traffic Policies

Note Layer 2 Ethernet traffic control only applies to Clean Access Servers operating in Virtual Gateway mode where Layer 2 Ethernet Control has been enabled on the CAS configuration page.

You can configure traffic policies for all the default roles already present in the system (Unauthenticated, Temporary, Quarantine). You will need to create normal login user roles first before you can configure traffic policies for them (see Chapter 6, "User Management: Configuring User Roles and Local Users.")

1. Go to **User Management > User Roles > Traffic Control > Ethernet**. The list of Layer 2 Ethernet traffic control policies for all roles appears (Figure 8-2).

Figure 8-9 Layer 2 Ethernet Traffic Control Policies



2. Select either **Allow** or **Block** from the **Action dropdown** menu.
3. Specify the type of Layer 2 Ethernet traffic to either allow or block in the **Protocol** dropdown menu.

Note Except for allowing all Layer 2 traffic, only the "IBM Systems Network Architecture (SNA)" protocol is available in Cisco NAC Appliance. Additional preset options may become available with future releases through the Cisco NAC Appliance update service on the Clean Access Manager.

4. Click **Enable**.
5. Click **Add**.

After you "Add" a traffic control policy, the CAM automatically populates the Description column for the entry with the description of the option you specified in the **Protocol** dropdown menu.

Control Bandwidth Usage

Cisco NAC Appliance lets you control how much network bandwidth is available to users by role. You can independently configure bandwidth management using global forms in the CAM as needed for system user roles, or only on certain Clean Access Servers using local forms. However, the option must first be enabled on the CAS for this feature to work. You can also specify bandwidth constraints for each user within a role or for the entire role.

For example, for a CAM managing two CASs, you can specify all the roles and configure bandwidth management on some of the roles as needed (e.g. guest role, quarantine role, Temporary role, etc.). If bandwidth is only important in the network segment where CAS1 is deployed and not on the network segment where CAS2 is deployed, you can then turn on bandwidth management on CAS1 but not CAS2.

With bursting, you can allow for brief deviations from a bandwidth constraint. This accommodates users who need bandwidth resources intermittently (for example, when downloading and reading pages), while users attempting to stream content or transfer large files are subject to the bandwidth constraint.

By default, roles have a bandwidth policy that is unlimited (specified as -1 for both upstream and downstream traffic).

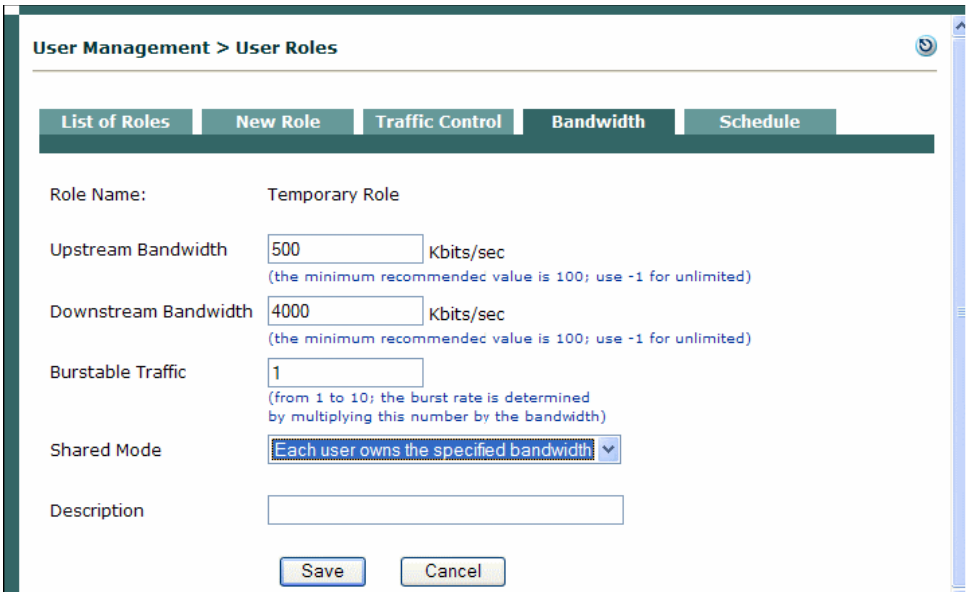
To configure bandwidth settings for a role:

1. First, enable bandwidth management on the CAS by going to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Bandwidth**.
2. Select **Enable Bandwidth Management** and click **Update**.

Note See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details on local bandwidth management.

3. From **User Management > User Roles > Bandwidth**, click the **Edit** icon next to the role for which you want to set bandwidth limitations. The **Bandwidth** form appears as follows:

Figure 8-10 Bandwidth Form for User Role



Note Alternatively, you can go to **User Management > User Roles > List of Roles** and click the **BW** icon next to the role.

4. Set the maximum bandwidth in kilobits per second for upstream and downstream traffic in **Upstream Bandwidth** and **Downstream Bandwidth**. Upstream traffic moves from the untrusted to the trusted network, and downstream traffic moves from the trusted to the untrusted network.
5. Enter a **Burstable Traffic** level from 2 to 10 to allow brief (one second) deviations from the bandwidth limitation. A **Burstable Traffic** level of 1 has the effect of disabling bursting.

   The **Burstable Traffic** field is a traffic burst factor used to determine the "capacity" of the bucket. For example, if the bandwidth is 100 Kbps and the **Burstable Traffic** field is 2, then the capacity of the bucket will be 100Kb*2=200Kb. If a user does not send any packets for a while, the user would have at most 200Kb tokens in his bucket, and once the user needs to send packets, the user will be able to send out 200Kb packets right away. Thereafter, the user must wait for the tokens coming in at the rate of 100Kbps to send out additional packets. This can be thought of as way to specify that for an average rate of 100Kbps, the peak rate will be approximately 200Kbps. Hence, this feature is intended to facilitate bursty applications such as web browsing.
6. In the **Shared Mode** field, choose either:
   - **All users share the specified bandwidth** – The setting applies for all users in the role. In this case, the total available bandwidth is a set amount. In other words, if a user occupies 80 percent of the available bandwidth, only 20 percent of the bandwidth will be available for other users in the role.
   - **Each user owns the specified bandwidth** – The setting applies to each user. The total amount of bandwidth in use may fluctuate as the number of online users in the role increases or decreases, but the bandwidth for each user is the same.
7. Optionally, type a **Description** of the bandwidth setting.
8. Click **Save** when finished.

The bandwidth setting is now applicable for the role and appears in the **Bandwidth** tab.

Note If bandwidth management is enabled, devices allowed via device filter without specifying a role will use the bandwidth of the Unauthenticated Role. See Global Device and Subnet Filtering, page 2-10 for details.

Configure User Session and Heartbeat Timeouts

Timeout properties enhance the security of your network by ensuring that user sessions are terminated after a configurable period of time. The are three main mechanisms for automated user timeout:

- Session Timer
- Heartbeat Timer
- Certified Device Timer (see Configure Certified Device Timer, page 11-14)

This section describes the Session and Heartbeat Timers.

Session Timer

The Session Timer is an absolute timer that is specific to the user role. If a Session Timer is set for a role, a session for a user belonging to that role can only last as long as the Session Timer setting. The Session Timer has a built-in value of 5 minutes that gets added to the configured session timeout value specific to the user role. A user session corresponding to a user role gets cleared at the end of configured session timeout + built-in 5 minute value. For example, if user A logs in at 1:00pm and user B logs in at 1:30pm, and if both belong to role Test with Session Timer set for 115 minutes, user A will be logged out at 3:00pm and user B will be logged out at 3:30pm. When session timeouts, the user is dropped regardless of connection status or activity.

Note If you have configured a RADIUS server, the RADIUS Session Timeout for user login is automatically enabled. The Timeout duration therefore occurs on a per user basis, depending on the user profile configured on the RADIUS server. Refer to RADIUS, page 7-6 for information on enabling RADIUS server authentication in Cisco NAC Appliance.

Heartbeat Timer

The Heartbeat Timer sets the number of minutes after which a user is logged off the network if unresponsive to ARP queries from the Clean Access Server. This feature enables the CAS to detect and disconnect users who have left the network (e.g. by shutting down or suspending the machine) without actually logging off the network. Note that the Heartbeat Timer applies to all users, whether locally or externally authenticated.

The connection check is performed via ARP query rather than by pinging. This allows the heartbeat check to function even if ICMP traffic is blocked. The CAS maintains an ARP table for its untrusted side which houses all the machines it has seen or queried for on the untrusted side. ARP entries for machines are timed out through normal ARP cache timeout if no packets are seen from the particular machine. If packets are seen, their entry is marked as fresh. When a machine no longer has a fully resolved entry in the CAS's ARP cache and when it does not respond to ARPing for the length of the Heartbeat Timer setting, the machine is deemed not to be on the network and its session is terminated.

In-Band (L2) Sessions

For In-Band configurations, a user session is based on the client MAC and IP address and persists until one of the following occurs:

- The user logs out of the network through either the web user logout page or the Agent logout option.
- An administrator manually removes the user from the network.
- The session times out, as configured in the Session Timer for the user role.
- The CAS determines that the user is no longer connected using the Heartbeat Timer and the CAM terminates the session.
- The Certified Device list is cleared (automatically or manually) and the user is removed from the network.

OOB (L2) and Multihop (L3) Sessions

The Session Timer works the same way for multi-hop L3 In-Band deployments as for L2 (In-Band or Out-of-Band) deployments.

For L3 deployments, user sessions are based on unique IP address rather than MAC address.

The Heartbeat Timer will not function in L3 deployments, and does not apply to OOB users. However, note that the HeartBeat Timer will work if the CAS is the first hop behind the VPN concentrator. This is because the VPN concentrator responds to the ARP queries for the IP addresses of its current tunnel clients.

Note When the Single Sign-On (SSO) feature is configured for multi-hop L3 VPN concentrator integration, if the user's session on the CAS times out but the user is still logged in on the VPN concentrator, the user will be able to log back into the CAS without providing a username/password, due to SSO.

Session Timer / Heartbeat Timer Interaction

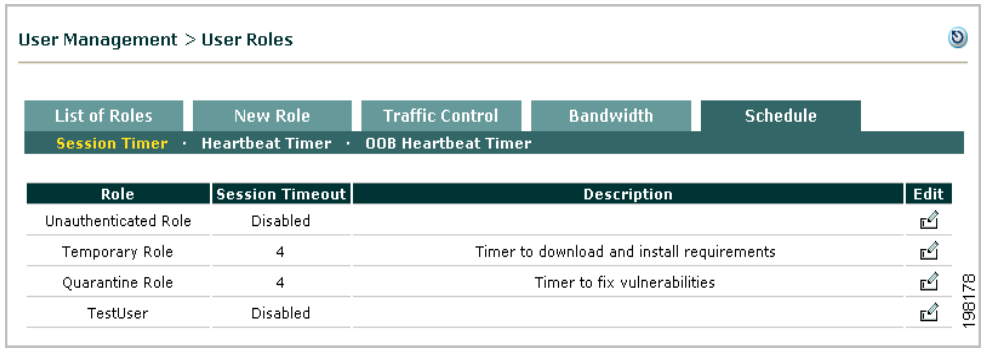
- If the Session Timer is zero and the Heartbeat Timer is not set—the user is not dropped from the Online Users list and will not be required to re-logon.
- If the Session Timer is zero and the Heartbeat Timer is set—the Heartbeat Timer takes effect.
- If the Session Timer is non-zero and the Heartbeat Timer is not set—the Session Timer takes effect.
- If both timers are set, the first timer to be reached will be activated first.
- If the user logs out and shuts down the machine, the user will be dropped from the Online Users list and will be required to re-logon.
- If the DHCP lease is much longer than the session timeout, DHCP leases will not be reused efficiently.

For additional details, see Interpreting Active Users, page 11-29.

Configure Session Timer (per User Role)

Step 1 Go to **User Management > User Roles > Schedule > Session Timer**.

Figure 8-11 Session Timer



Step 2 Click the **Edit** icon next to the role for which you want to configure timeout settings.

Step 3 Select the **Session Timeout** check box and type the number of minutes after which the user's session times out. The timeout clock starts when the user logs on, and is not affected by user activity. After the session expires, the user must log in again to continue using the network.

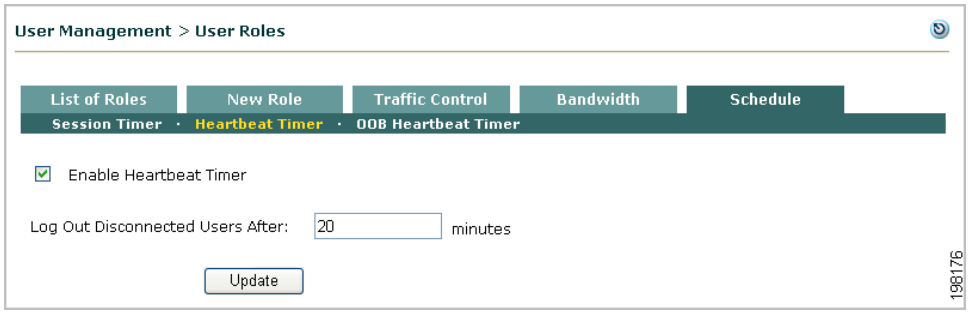
Step 4 Optionally, type a description of the session length limitation in the **Description** field.

Step 5 Click **Update** when finished.

Configure Heartbeat Timer (User Inactivity Timeout)

Step 1 Open the **Heartbeat Timer** form in the **Schedule** tab.

Figure 8-12 Heartbeat Timer



Step 2 Click the **Enable Heartbeat Timer** checkbox.

Step 3 Set the number of minutes after which a user is logged off the network if unreachable by connection attempt in the **Log Out Disconnected Users After** field.

Step 4 Click **Update** to save your settings.

Note that logging a user off the network does not remove them from the Certified Devices List. However, removing a user from the Certified Devices List also logs the user off the network. An administrator can drop users from the network individually or terminate sessions for all users at once. For additional details see Clear Certified or Exempt Devices Manually, page 11-13 and Interpreting Event Logs, page 13-4.

Note The Agent does not send a logout request to the CAS when the client machine is shut down based on Cisco NAC Appliance session-based connection setup.

Configure OOB Heartbeat Timer (per User Role)

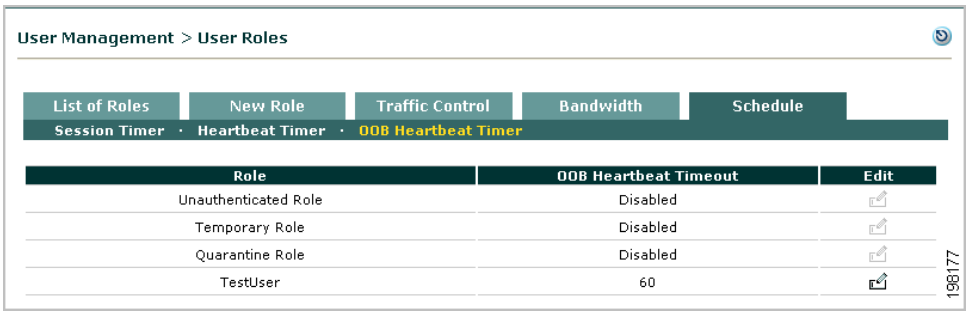
Step 1 Go to **User Management > User Roles > Schedule > OOB Heartbeat Timer**.

Note The OOB Heartbeat Timer is disabled by default.

Note In order to configure OOB Heartbeat Timer, you *must* also enable Out-of-Band Logoff. See Configure Out-of-Band Logoff, page 9-6.

Caution To avoid disconnecting users currently logged into the Cisco NAC Appliance network, Cisco strongly recommends disabling the Out-of-Band Heartbeat Timer during a planned network outage, as changing this setting could kick all current users from the Out-of-Band Online Users list.

Figure 8-13 OOB Heartbeat Timer



Step 2 Click the **Edit** icon next to the role for which you want to configure Heartbeat timeout settings.

Step 3 Select the **OOB Heartbeat Timeout** check box and type the number of minutes after which the user's session times out. The minimum time that can be configured is two minutes. The timeout clock starts when the user logs on, and is not affected by user activity. The Heartbeat timer kicks the user after the session expires, when there is no communication between the client and the CAS. After the session

expires, the user must log in again to continue using the network. For example, if the timer is set for 5 minutes, and the user removes the system from the network for 6 minutes, the user must log in again to use the network.

Step 4 Click **Update** to enable the Heartbeat Timeout.

Configure Policies for Agent Temporary and Quarantine Roles

This section demonstrates typical traffic policy and session timeout configuration needed to:

- Configure Agent Temporary Role, page 8-19
- Configure Network Scanning Quarantine Role, page 8-21

Configure Agent Temporary Role

Users who fail a system check are assigned to the Agent Temporary role. This role is intended to restrict user access to only the resources needed to comply with the Agent requirements.

Unlike Quarantine roles, there is only one Agent Temporary role in the Cisco NAC Appliance system. The role can be fully edited, and is intended as single point for aggregating the traffic control policies that allow users to access required installation files. If the Temporary role is deleted, the Unauthenticated role is used by default. The name of the role that is used for the Temporary role (in addition to the version of the Agent) is displayed under **Device Management > Clean Access > Clean Access Agent > Distribution**.

Both session timeout and traffic policies need to be configured for the Temporary role. The Temporary role has a default session timeout of 4 minutes, which can be changed as described below. The Temporary and quarantine roles have default traffic control policies of Block All traffic from the untrusted to the trusted side. Keep in mind that while you associate requirements (required packages) to the normal login roles that users attempt to log into, clients will need to meet those requirements while still in the Temporary role. Therefore, traffic control policies need to be added to the Temporary role to enable clients to access any required software installation files from the download site(s).

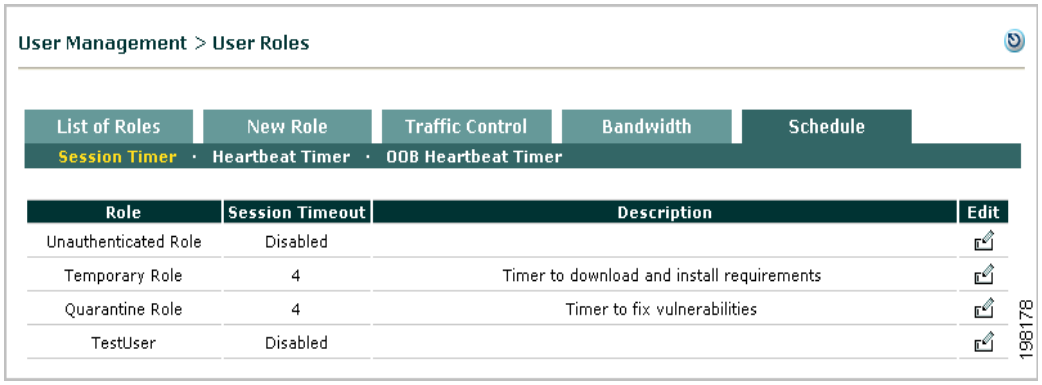
Note If the user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example), and the **Logoff NAC Agent users from network on their machine logoff or shutdown after <*x*> secs** option in the CAM **Device Management > Clean Access > General Setup > Agent Login** web console page has not been enabled, the client machine remains in the Temporary role until the Session Timer expires and the user is given the opportunity to perform login/remediation again.

Configuring Agent-Based Posture Assessment, page 9-39 provides complete details on Agent Requirement configuration. See also User Role Types, page 6-3 for additional information.

Configure Session Timeout for the Temporary Role

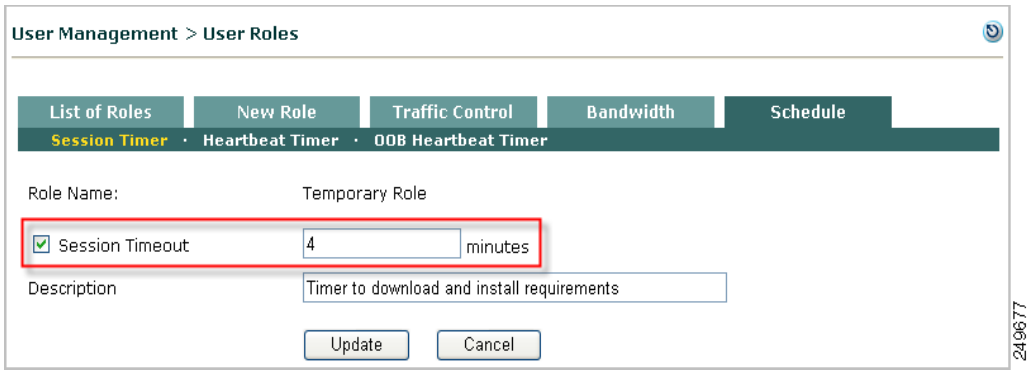
1. Go to **User Management > User Roles> Schedule**.
2. The **Session Timer** list appears.

Figure 8-14 Schedule Tab



3. Click the **Edit** icon for the Temporary Role.
4. The **Session Timer** form for the Temporary Role appears (Figure 8-15).

Figure 8-15 Session Timer—Temporary Role

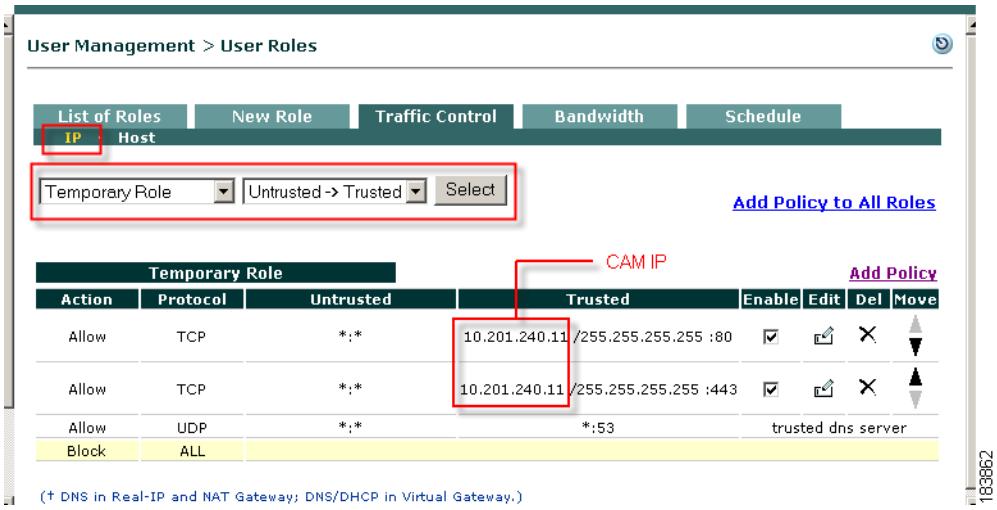


5. Click the **Session Timeout** checkbox.
6. Type the number of minutes for the user session to live (default is 4 minutes). Choose a value that allows users to download required files to patch or configure their systems.
7. Optionally, type a **Description** for the session timeout requirement.
8. Click **Update**. The Temporary role will display the new time in the **Session Timer** list.

Configure Traffic Control Policies for the Temporary Role

9. From **User Management > User Roles**, click the **Traffic Control** tab. This displays **IP** traffic policy list by default.
10. Choose **Temporary Role** from the role dropdown and leave **Untrusted->Trusted** for the direction and click **Select**. This displays all IP policies for the Temporary role.

Figure 8-16 IP Traffic Policies—Temporary Role



11. To configure an **IP** policy, click the **Add Policy** link next to the Temporary role. For example, if you are providing required software installation files yourself (e.g. via a File Distribution requirement for a file on the CAM), set up an Untrusted->Trusted IP-based traffic policy that allows the Temporary role access to port 443 (HTTPS) of the CAM (for example, 10.201.240.11 /255.255.255.255:443). If you want users to be able to correct their systems using any other external web pages or servers, set up permissions for accessing those web resources. For further details on the **Add Policy** page, see Add IP-Based Policy, page 8-4.
12. To configure **Host** policies, click the **Host** link at the top of the **Traffic Control** tab. Configure host-based traffic policies enabling access to the servers that host the installation files, as described in the following sections:
    - Enable Default Allowed Hosts, page 8-9
    - Add Allowed Host, page 8-10
    - Adding Traffic Policies for Default Roles, page 8-27

Configure Network Scanning Quarantine Role

See Chapter 12, "Configuring Network Scanning" for complete details on network scanning configuration.

Cisco NAC Appliance can assign a user to a quarantine role if it discovers a serious vulnerability in the client system. The role is a mechanism intended to give users temporary network access to fix their machines. Note that quarantining vulnerable users is optional. Alternatives include blocking the user or providing them with a warning. If you do not intend to quarantine vulnerable users, you can skip this step.

Create Additional Quarantine Role

By default, the system provides a default Quarantine role with a session time out of 4 minutes that only needs to be configured with traffic policies. The following describes how to create an additional quarantine role, if multiple quarantine roles are desired.

1. Go to **User Management > User Roles > New Role**.

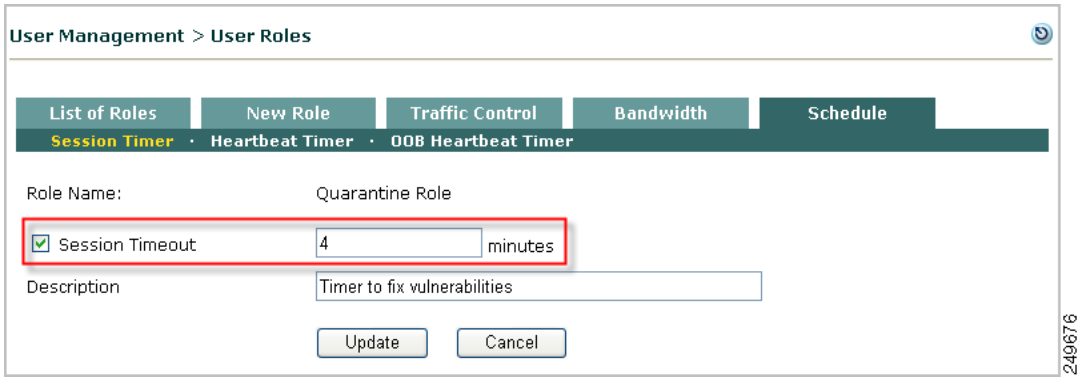
2. Type a **Role Name** and **Role Description** of the role. For a quarantine role that will be associated with a particular login role, it may be helpful to reference the login role and the quarantine type in the new name. For example, a quarantine role associated with a login role named "R1" might be "R1-Quarantine."
3. In the **Role Type** list, choose **Quarantine Role**.
4. Configure any other settings for the role as desired. Note that, other than name, description, and role type, other role settings can remain at their default values. (See Adding a New User Role, page 6-7 for details.)
5. Click the **Create Role** button. The role appears in the **List of Roles** tab.

Configure Session Timeout for Quarantine Role

By default, the system provides a default Quarantine role with a session time out of 4 minutes. The following steps describe how to configure the session timeout for a role.

1. Go to **User Management > User Roles > Schedule > Session Timer**.
2. Click the **Edit** icon next to the desired quarantine role.
3. The **Session Timer** form for the quarantine role appears:

Figure 8-17 Session Timer—Quarantine Role



4. Click the **Session Timeout** check box.
5. Type the number of minutes for the user session to live. Choose an amount that allows users enough time to download the files needed to fix their systems.
6. Optionally, type a **Description** for the session timeout requirement.
7. Click **Update**. The new value will appear in the **Session Timeout** column next to the role in the **List of Roles** tab.

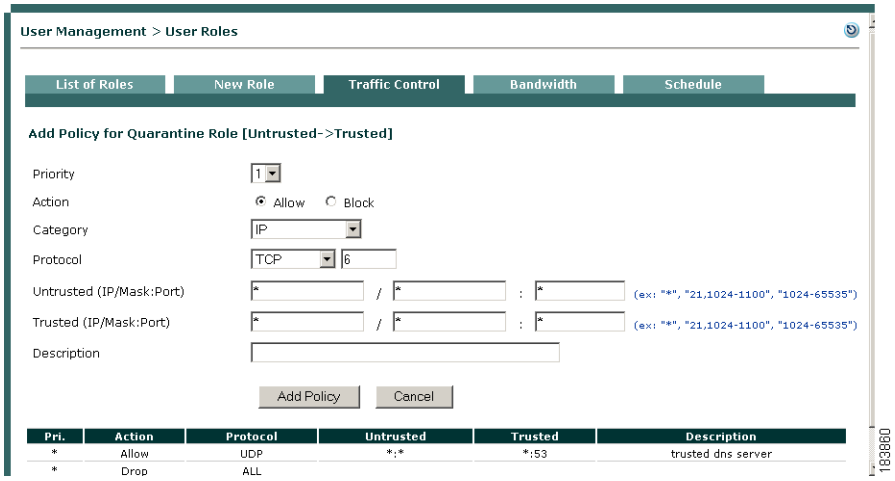
Setting these parameters to a relatively small value helps the CAS detect and disconnect users who have restarted their computers without logging out of the network. Note that the Session Timer value you enter here may need to be refined later, based on test scans and downloads of the software you will require.

Note The connection check is performed by ARP message; if a traffic control policy blocks ICMP traffic to the client, heartbeat checking still works.

Configure Traffic Control Policies for the Quarantine Role

1. From **User Management > User Roles > List of Roles**, click the **Policies** icon next to the role (or you can click the **Traffic Control** tab, choose the quarantine role from the dropdown menu and click **Select**).
2. Choose the **Quarantine Role** from the role dropdown, leave **Untrusted->Trusted** for the direction and click **Select**. This displays all IP policies for the Quarantine role.
3. To configure an **IP** policy, click the **Add Policy** link next to the Quarantine role.

Figure 8-18 Add Policy—Quarantine Role



4. Configure fields as described in Add IP-Based Policy, page 8-4.
   - If you are providing required software installation files from the CAM (e.g. via network scanning Vulnerabilities page), set up an Untrusted->Trusted IP-based traffic policy that allows the Quarantine role access to port 80 (HTTP) of the CAM (for example, 10.201.240.11 /255.255.255.255:80).
   - If you want users to be able to correct their systems using any other external web pages or servers, set up permissions for accessing those web resources. See also Adding Traffic Policies for Default Roles, page 8-27.
5. To configure **Host** policies, click the **Host** link for the Quarantine role at the top of the **Traffic Control** tab. Configure host-based traffic policies enabling access to the servers that host the installation files, as described in the following sections:
   - Enable Default Allowed Hosts, page 8-9
   - Add Allowed Host, page 8-10
   - Adding Traffic Policies for Default Roles, page 8-27

After configuring the quarantine role, you can apply it to users by selecting it as their quarantine role in the **Block/Quarantine users with vulnerabilities in role** option of the **General Setup** tab. For details, see Client Login Overview, page 1-6.

When finished configuring the quarantine role, load the scan plugins as described in Load Nessus Plugins into the Clean Access Manager Repository, page 12-6.

Example Traffic Policies

This section describes the following:

- Allowing Authentication Server Traffic for Windows Domain Authentication, page 8-24
- Allowing Traffic for Enterprise AV Updates with Local Servers, page 8-24
- Allowing Gaming Ports, page 8-24
- Adding Traffic Policies for Default Roles, page 8-27

Allowing Authentication Server Traffic for Windows Domain Authentication

If you want users on the network to be able to authenticate to a Windows domain prior to authenticating to the Cisco NAC Appliance, the following minimum policies allow users in the Unauthenticated role access to AD (NTLM) login servers:

Allow TCP *:* Server/255.255.255.255: 88

Allow UDP *:* Server/255.255.255.255: 88

Allow TCP *:* Server/255.255.255.255: 389

Allow UDP *:* Server/255.255.255.255: 389

Allow TCP *:* Server/255.255.255.255: 445

Allow UDP *:* Server/255.255.255.255: 445

Allow TCP *:* Server/255.255.255.255: 135

Allow UDP *:* Server/255.255.255.255: 135

Allow TCP *:* Server/255.255.255.255: 3268

Allow UDP *:* Server/255.255.255.255: 3268

Allow TCP *:* Server/255.255.255.255: 139

Allow TCP *:* Server/255.255.255.255: 1025

Allowing Traffic for Enterprise AV Updates with Local Servers

In order to allow definition updates for enterprise antivirus products, such as Trend Micro OfficeScan, the Temporary role needs to be configured to allow access to the local server for automatic AV definition updates.

For Trend Micro OfficeScan, the Temporary role policy needs to allow access to the local server with AutoPccP.exe. The Agent calls the Trend client locally, and the Trend client in turn runs the AutoPccP.exe file either on a share drive (located at \\<trendserverip\ofcscan\Autopccp.exe) or through HTTP (depending on your TrendMicro configuration) and downloads the AV patches.

Allowing Gaming Ports

To allow gaming services, such as Microsoft Xbox Live, Cisco recommends creating a gaming user role and to add a filter for the device MAC addresses (under **Device Management > Filters > Devices > New**) to place the devices into that gaming role. You can then create traffic policies for the role to allow traffic for gaming ports.

Microsoft Xbox

The following are suggested policies to allow access for Microsoft Xbox ports:

- Kerberos-Sec (UDP); Port 88; UDP; Send Receive
- DNS Query (UDP); Port 53; Send 3074 over UDP/tcp
- Game Server Port (TCP): 22042
- Voice Chat Port (TCP/UDP): 22043-22050
- Peer Ping Port (UDP): 13139
- Peer Query Port (UDP): 6500

Other Game Ports

Table 8-1 shows suggested policies to allow access for other game ports (such as PlayStation).

Table 8-1 Traffic Policies for Other Gaming Ports [1]

Protocol Port	Protocol
2300-2400	UDP
4000	TCP, UDP
4000	TCP, UDP
80	TCP
2300	UDP
6073	UDP
2302-2400	UDP
33334	UDP
33335	TCP
6667	TCP
3783	TCP
27900	TCP
28900	TCP
29900	TCP
29901	TCP
27015	TCP
2213 + 1 for each client (i.e. first computer is 2213, second computer is 2214, third computer is 2215, etc.)	TCP
6073	TCP
2302-2400	UDP
27999	TCP
28000	TCP
28805-28808	TCP

Table 8-1 Traffic Policies for Other Gaming Ports [1]

Protocol Port	Protocol
9999	TCP
47624	TCP
2300-2400	TCP
2300-2400	UDP
6073	UDP
2302-2400	UDP
47624	TCP
2300-2400	TCP
2300-2400	UDP
5120-5300	UDP
6500	UDP
27900	UDP
28900	UDP
3782	TCP
3782	UDP
27910	TCP, UDP
6073	UDP
2302-2400	UDP
47624	TCP
2300-2400	TCP
2300-2400	UDP
4000	TCP
7777	TCP, UDP
4000	TCP
27015-27020	TCP
6667	TCP
28800-29000	TCP

1. See also http://www.us.playstation.com/support.aspx?id=installation/networkadaptor/415013907.html for additional details.

For additional details, see:

- Device Filters and Gaming Ports, page 2-17
- http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q16
- Adding a New User Role, page 6-7

Adding Traffic Policies for Default Roles

Create Untrusted -> Trusted traffic policies for the default roles (Unauthenticated, Temporary, and Quarantine) to allow users access to any of the resources described below.

Unauthenticated Role

If customizing the web login page to reference logos or files on the CAM or external URL, create IP policies to allow the Unauthenticated role HTTP (port 80) access to the CAM or external server. (See also Upload a Resource File, page 5-13 and Create Content for the Right Frame, page 5-11 for details.)

Agent Temporary Role

- If providing definition updates for enterprise antivirus products, allow access to the local update server so that the Agent can trigger a live update (see Allowing Traffic for Enterprise AV Updates with Local Servers, page 8-24).

Note This behavior is only applicable to the Cisco NAC Agent because the Cisco NAC Web Agent does not support automatic remediation.

- If providing required software packages from the CAM (e.g, via File Distribution), create IP policies to allow Temporary role access to port 443 (HTTPS) of the CAM. Make sure to specify IP address/subnet mask to allow access only to the CAM (for example, 10.201.240.11/255.255.255.255:443).
- Enable Default Host Policies and Trusted DNS Server and/or create new allowed Host policies to allow users access to update sites (see Enable Default Allowed Hosts, page 8-9).
- Set up any additional traffic policies to allow users in the Temporary role access to external web pages or servers (for example, see Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 9-11).

Quarantine Role

- If providing required software packages from the CAM (e.g. via network scanning Vulnerabilities page), create IP policies to allow the Quarantine role access to port 443 (HTTPS) of the CAM. Make sure to specify the IP address and subnet mask to allow access only to the CAM (for example, 10.201.240.11 /255.255.255.255:443).
- Enable Default Host Policies and Trusted DNS Server and/or create new allowed Host policies to allow users access to update sites (see Enable Default Allowed Hosts, page 8-9).
- Set up any additional traffic policies to allow users in the Quarantine role access to external web pages or servers for remediation.

Table 8-2 summarize resources, roles and example traffic policies for system roles

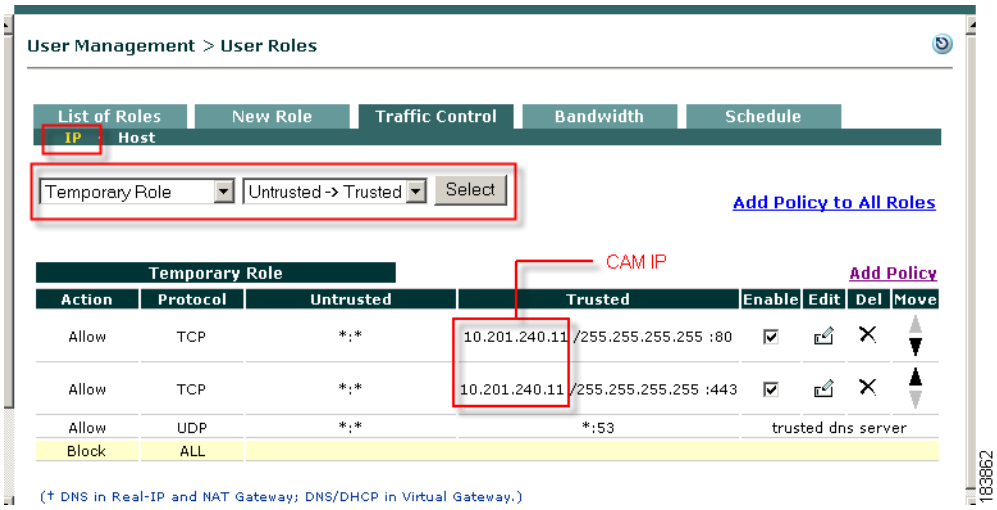
Table 8-2 Typical Traffic Policies for Roles

Resource	Role	Example Policies (Untrusted -> Trusted)
IP-Based Traffic Policies		
Logo/right-frame content for Login page (logo.jpg, file.htm)	Unauthenticated	**IP (Files on CAM or External Server):** Allow TCP *.* <*CAM_IP_address* or *external_server_IP_address*> / 255.255.255.255: https (443)
User Agreement Page (UAP.htm)		
Redirect URL after blocked access (block.htm) — optional		
Network Policy Page (AUP.htm)	Temporary	
File Distribution Requirement file (Setup.exe)		
Vulnerability Report file (fixsteps.htm; stinger.exe)	Quarantine	
Host-Based Traffic Policies		
Enable Trusted DNS Server	All roles using Host policies	**Trusted DNS Server:** e.g. 63.93.96.20, or * (Any DNS Server)
Link Distribution Requirement (external website)	Temporary	**Default Host:** windowsupdate.com, or **Custom Host:** database.clamav.net (equals)
Vulnerability Report (link to external website)	Quarantine	
Other		
Proxy server in environment	Any role with access via proxy	**IP:** <*proxy_IP_address*>/255.255.255.255:https(443) **Host:** proxy-server.com (equals)
Full network access	Normal Login Role	Allow ALL TRAFFIC * /*

For further details, see:

- Upload a Resource File, page 5-13
- Create Content for the Right Frame, page 5-11
- Create File Distribution/Link Distribution/Local Check Requirement, page 9-80
- Configure Vulnerability Handling, page 12-13

Figure 8-19 Example Traffic Policies for File Distribution Requirement (File is on CAM)



Troubleshooting Host-Based Policies

For host-based policies, the CAS needs to see DNS responses in order to allow the traffic. If having trouble with host-based policies, check the following:

- Make sure allowed hosts are enabled.
- Make sure a DNS server has been correctly added to the list of DNS servers to track (you can also add an asterisk ("*") to track any DNS server).
- Make sure the DNS server is on the trusted interface of the CAS. If the DNS server is on the untrusted side of the CAS, the CAS never sees the DNS traffic.
- Make sure DNS reply traffic is going through the CAS. For example, ensure there is no alternate route for return traffic (i.e. trusted to untrusted) where traffic goes out through CAS but does not come back through the CAS. This can be tested by adding a "Block ALL" policy to the "Trusted to Untrusted" direction for the Unauthenticated or Temporary Role. If DNS, etc. still succeeds, then there is an alternate path.
- Make sure the DNS server listed for the client is correct.
- Make sure proxy settings are correct for the client (if proxy settings are required)
- Check **Device Management > CCA Servers > Manage [CAS_IP] > Filters > Roles > Allowed Hosts > View Current IP Address List** to see the list of current IPs that are being tracked through the host based policies. If this list is empty, users will see a security message.



Configuring Cisco NAC Appliance for Agent Login and Client Posture Assessment

This chapter describes how to configure Agent distribution and installation for client machines, as well as configure client posture assessment in the Cisco NAC Appliance system.

- Overview, page 9-1
- Add Default Login Page, page 9-3
- Configure Agent Roles and User Profiles, page 9-3
- Require Agent Login for Client Machines, page 9-3
- Retrieving Cisco NAC Appliance Updates, page 9-12
- Setting Up Agent Distribution/Installation, page 9-17
- Configuring Agent-Based Posture Assessment, page 9-39
- Post-Configuration and Agent Maintenance on the CAM, page 9-100

Overview

The Cisco NAC Agent and Cisco NAC Web Agent provide local posture assessment and remediation for client machines.

Users download and install the Cisco NAC Agent (read-only client software), which can check the host registry, processes, applications, and services. The Agent can be used to perform antivirus or antispyware definition updates, distribute files uploaded to the Clean Access Manager, distribute website links to websites in order for users to download files to fix their systems, or simply distribute information/instructions.

Unlike the Cisco NAC Agent, the Cisco NAC Web Agent is not “persistent,” thus it only exists on the client machine long enough to accommodate a single user session. Instead of downloading and installing an Agent application, once the user opens a browser window, logs in to the NAC Appliance web login page, and chooses to launch the temporal Cisco NAC Web Agent, a self-extracting Agent installer downloads files to the client machine’s temporary directory, performs posture assessment/scans the system to ensure security compliance, and report compliance status back to the Cisco NAC Appliance system. For more information on Cisco NAC Appliance Agents, see Chapter 10, “Cisco NAC Appliance Agents.”

Agent posture assessment is configured in the CAM by creating requirements based on rules and (optionally) checks, then applying the requirements to user roles/client operating systems. For an illustrated overview, see Figure 9-10 on page 9-41.

Note Most requirement remediation actions (like Windows Updates and AV/AS support updates) require the user to have administrator privileges on the client machine. Therefore, Cisco recommends you ensure that users of client machines undergoing posture assessment and remediation have administrator-level privileges.

Users in L3 Deployments

Cisco NAC Appliance supports multi-hop L3 deployment and VPN concentrator/L3 access from the Agent. This enables clients to discover the CAS when the network configuration puts clients one or more L3 hops away from the CAS (instead of in L2 proximity). You must Enable L3 Support on the CAS and ensure there is a valid Discovery Host for the Agent to function in multihop L3 environments or behind a Cisco VPN concentrator.

Distribution

The Cisco NAC Agent Installation files and the Cisco NAC Web Agent are part of the Clean Access Manager software and are automatically published to all Clean Access Servers. To distribute the Agent to clients for initial installation, you require the use of the Agent for a user role and operating system in the **General Setup > Agent Login** tab. The CAS then distributes the Agent Setup file when the client requests the Agent. (This behavior does not apply to the Cisco NAC Web Agent.) If the CAS has an outdated version of the Agent, the CAS acquires the newest version available from the CAM before distributing it to the client.

Auto Upgrade

By configuring Agent auto-upgrade in the CAM, you can allow users to automatically upgrade upon login to the latest version of the Agent available on the CAM. With the Cisco NAC Web Agent, users automatically download the latest version of the temporal Agent available on the CAM.

Installation

You can configure the level of user interaction required when users initially install the Agent.

Out-of-Band Users

Because Out-of-Band users only encounter the Agent during the time they are In-Band for authentication and certification, Agent configuration is the same for In-Band and Out-of-Band users.

Rules and Checks

With pre-configured Cisco checks and rules, or custom checks and rules that you configure, the Agent can check if any application or service is running, whether a registry key exists, and/or the value of a registry key. Cisco pre-configured rules provide support for Critical Windows OS hotfixes.

Agent Updates

Through the **Updates** page of your CAM web console, Cisco tracks and provides multiple updates per hour, including the latest versions of Cisco NAC Agent installers and Cisco NAC Web Agent installation packages as they become available. See Retrieving Cisco NAC Appliance Updates, page 9-12 for complete details.

Agent Configuration Steps

The basic steps needed to configure Agent distribution, installation, and posture assessment are:

Step 1 Add Default Login Page, page 9-3

Step 2 Configure Agent Roles and User Profiles, page 9-3

Step 3 Require Agent Login for Client Machines, page 9-3

Step 4 Retrieving Cisco NAC Appliance Updates, page 9-12

Step 5 Setting Up Agent Distribution/Installation, page 9-17

Step 6 Configuring Agent-Based Posture Assessment, page 9-39

Add Default Login Page

In order for both web login users and Agent users to obtain the list of authentication providers, a login page must be added and present in the system in order for user to authenticate via the Agent. See Add Default Login Page, page 5-3 to quickly add the default user login page.

Note For L3 OOB deployments, you must also Enable Web Client for Login Page, page 5-5.

Configure Agent Roles and User Profiles

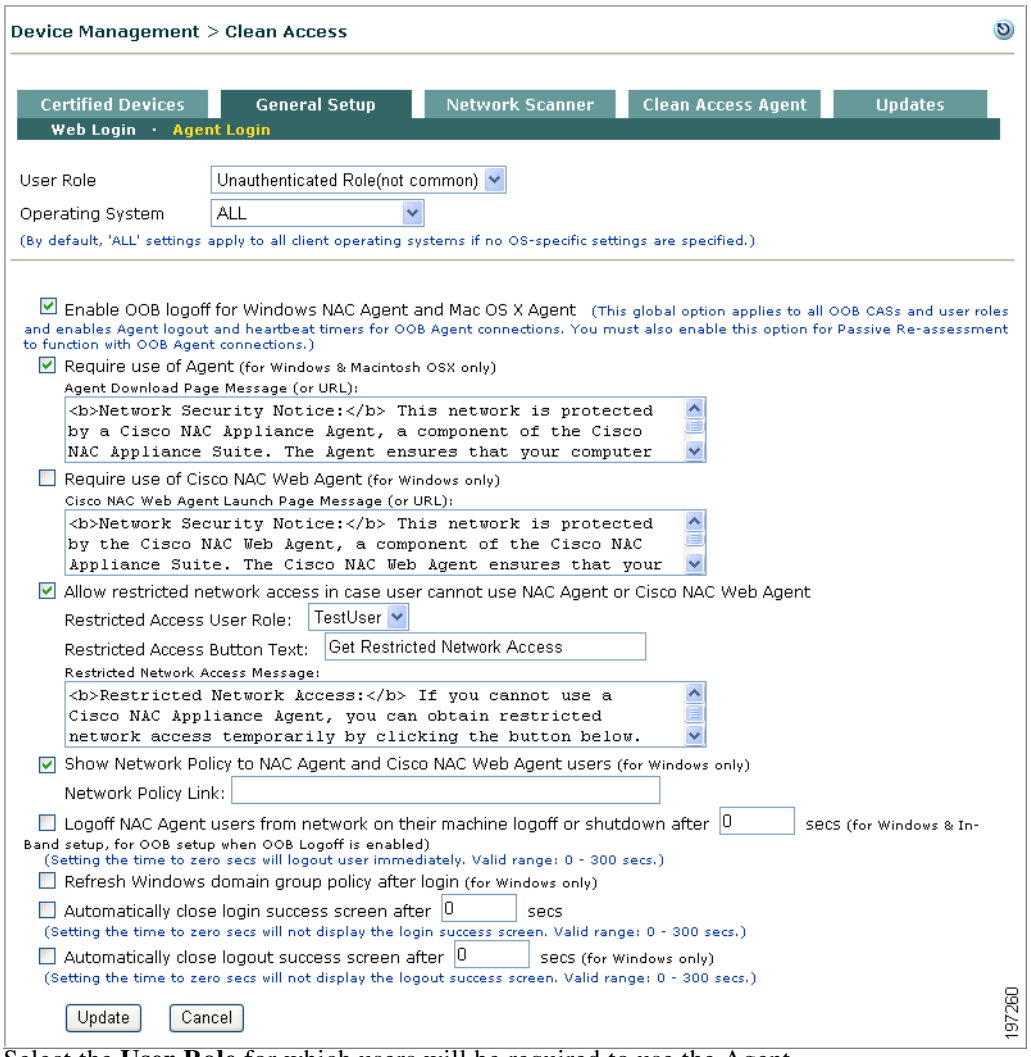
In order for Agent users to log in to Cisco NAC Appliance, you must ensure that user login roles and user profiles are configured in the system. See Create User Roles, page 6-2 and Create Local User Accounts, page 6-15 to add user roles and individual user login profiles in Cisco NAC Appliance.

Require Agent Login for Client Machines

Requiring the use of the Agent is configured per user role and operating system. When an Agent is required for a role, users in that role are forwarded to the Agent download page (Figure 9-2) after authenticating for the first time using web login. The user is then prompted to download and run the Agent installation file or launch the Cisco NAC Web Agent. At the end of the installation, the user is prompted to log into the network using the Agent. (Cisco NAC Web Agent users are automatically connected to the network as long as their client machine meets Agent Requirements configured for the user role.)

Step 1 Go to **Device Management > Clean Access > General Setup > Agent Login** (Figure 9-1).

Figure 9-1 General Setup


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Web Login · Agent Login
User Role
Unauthenticated Role(not common)
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
Enable OOB logoff for Windows NAC Agent and Mac OS X Agent (This global option applies to all OOB CASs and user roles and enables Agent logout and heartbeat timers for OOB Agent connections. You must also enable this option for Passive Re-assessment to function with OOB Agent connections.)
Require use of Agent (for Windows & Macintosh OSX only)
Agent Download Page Message (or URL):
Network Security Notice: This network is protected by a Cisco NAC Appliance Agent, a component of the Cisco NAC Appliance Suite. The Agent ensures that your computer
Require use of Cisco NAC Web Agent (for Windows only)
Cisco NAC Web Agent Launch Page Message (or URL):
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco NAC Appliance Suite. The Cisco NAC Web Agent ensures that your
Allow restricted network access in case user cannot use NAC Agent or Cisco NAC Web Agent
Restricted Access User Role: TestUser
Restricted Access Button Text: Get Restricted Network Access
Restricted Network Access Message:
Restricted Network Access: If you cannot use a Cisco NAC Appliance Agent, you can obtain restricted network access temporarily by clicking the button below.
Show Network Policy to NAC Agent and Cisco NAC Web Agent users (for Windows only)
Network Policy Link:
Logoff NAC Agent users from network on their machine logoff or shutdown after 0 secs (for Windows & In-Band setup, for OOB setup when OOB Logoff is enabled)
(Setting the time to zero secs will logout user immediately. Valid range: 0 - 300 secs.)
Refresh Windows domain group policy after login (for Windows only)
Automatically close login success screen after 0 secs
(Setting the time to zero secs will not display the login success screen. Valid range: 0 - 300 secs.)
Automatically close logout success screen after 0 secs (for Windows only)
(Setting the time to zero secs will not display the logout success screen. Valid range: 0 - 300 secs.)
Update
Cancel
197260

Step 2 Select the **User Role** for which users will be required to use the Agent.

Step 3 Select an **Operating System** from the items available in the dropdown menu.

Note Make sure the Operating System is correctly configured for the role to ensure the Agent download page and/or Cisco NAC Web Agent launch page is properly pushed to users.

Step 4 If you want to require users to log in to the Cisco NAC Appliance system using the Cisco NAC Agent, click the checkbox for **Require use of Agent**. For information on Distribution settings, see Agent Distribution, page 9-18. For more information on the Cisco NAC Agent and user dialog examples, see Cisco NAC Agent, page 10-1.

Step 5 If you want to require users to log in to the NAC Appliance system using the Cisco NAC Web Agent, click the checkbox for **Require use of Cisco NAC Web Agent**. For more information on the Cisco NAC Web Agent and user dialog examples, refer to Cisco NAC Web Agent, page 10-25.

Note The **Require use of Agent** and **Require use of Cisco NAC Web Agent** options are *not* mutually exclusive. If you choose to enable both options, both choices appear to users when they are directed to the Login Page,

Step 6 You can leave the default messages, or optionally type your own HTML message in the **Agent Download Page Message (or URL)** and/or **Cisco NAC Web Agent Launch Page Message (or URL)** text fields.

Step 7 Click **Update**.

Note For additional details on configuring the General Setup page, see Client Login Overview, page 1-6.

Agent users logging in for the first time with the web login page see the Agent Download Page, as shown in Figure 9-2.

Figure 9-2 Agent Download Page


Cisco NAC Web Agent Download
Page
Safety
Tools
Network Security Notice: This network is protected by a Cisco NAC Appliance Agent, a component of the Cisco NAC Appliance Suite. The Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please use the Agent to log in to the network.
If you don't have the Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.
If you have already downloaded and installed the Agent, please close this window and right-click the Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.
Launch Cisco NAC Windows Agent 4.9.5.6
Note: If you are already running the NAC Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the

Cisco NAC Web Agent users logging in for the first time with the web login page see the Cisco NAC Web Agent Launch Page, as shown in Figure 9-3.

Figure 9-3 Cisco NAC Web Agent Launch Page


Cisco NAC Web Agent Download
Page
Safety
Tools
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco NAC Appliance Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please launch Cisco NAC Web Agent by clicking the button below.
Launch Cisco Web Agent 4.9.5.3
Network Security Notice: This network is protected by a Cisco NAC Appliance Agent, a component of the Cisco NAC Appliance Suite. The Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please use the Agent to log in to the network.
If you don't have the Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.

Configure Out-of-Band Logoff

Caution To avoid disconnecting users currently logged into the Cisco NAC Appliance network, Cisco strongly recommends disabling the Out-of-Band Heartbeat Timer during a planned network outage, as changing this setting could kick all current users from the Out-of-Band Online Users list.

The Out-of-Band logoff feature is disabled in Cisco NAC Appliance by default and is not applicable for the Cisco NAC Web Agent or web login user sessions.

Feature Benefits

- Out-of-Band Logoff can be used to monitor and to track users in OOB user list.
- This feature allows the Agent on the client machines to initiate the log-off process in an Out-of-Band deployment.
- Out-of-Band Logout is available in the agent tray icon and is useful for the shared environments when one user needs to logout of CAM for another user to be logged into CAM to gain access to a different network.
- Out-of-Band Logoff is useful when users are connected behind an IP Phone. When the users disconnect, the managed switch will not send a linkdown trap to the CAM prompting to remove the user from the Out-of-Band Online Users list. You can enable OOB Heartbeat timer, so that after the timer expires, users who are no longer on the network are removed.

Feature Dependencies - Mandatory

- For Out-of-Band Logoff to function, both the CAM/CAS should be installed with Release 4.8 or later and the client machine should be running the corresponding Cisco NAC Agent version, that is 4.8.0.32 or later.

- In order for Agent Out-of-Band Logoff to function correctly in a deployment requiring VLAN change based on user role (in both Layer 3 Out-of-Band deployments and Layer 2 Out-of-Band environments where the client machine IP address is refreshed following login), you must enable the VLAN change detection option as per the guidelines in Configure Access to Authentication VLAN Change Detection, page 3-67.

  Ensure that the **VLANdetectWithoutUI** parameter is enabled in the **NACAgentCFG.xml** Agent configuration file accordingly. (See Cisco NAC Agent XML Configuration File Settings, page 9-23.) This is enabled for refreshing the IP address in the Authentication VLAN after CAM clears the user and moves the user from Access VLAN to Authentication VLAN. This is used when OOB logoff feature is used with Windows logoff.
- If you want to enforce Agent Passive Re-assessment (PRA) for your Cisco NAC Appliance Out-of-Band deployment, you *must* enable the Out-of-Band Logoff function. For more information on Agent Passive Reassessment, see Adding a New User Role, page 6-7 and Modifying an Existing Temporary, Quarantine, or Login Role, page 6-14.

Note Passive Re-Assessment can be enabled only for Cisco NAC Agent. The Mac OS X Agent does not support PRA.

- Prior to Release 4.8, deployments using Access Control Lists (ACLs), Layer 3 Out-of-Band Real-IP Gateway mode, and CAS certificates based on the untrusted network IP address need to block UDP ports 8905/8906 to ensure that the access VLAN clients could not communicate with the untrusted side of the CAS and attempt another login. Policy Based Routing can be used to ensure that all non-NAC Authentication VLAN traffic is sent to the trusted side IP address of the CAS.

  In Cisco NAC Appliance Release 4.8 and later, if ACLs block access to the CAS, then the OOB Logoff feature will not function as designed. Cisco NAC Appliance network administrators must leave UDP ports 8905/8906 open on network switches to ensure the CAS trusted interface can communicate during the following OOB scenarios: OOB Heartbeat Timers, OOB Logout, and Passive Re-assessment. Use Policy Based Routing to ensure that all non-Authentication client network traffic is forced to the CAS trusted interface.
- Verify that the port profile(s) to which reconnecting users are assigned specify the *Authentication VLAN* for the **Change to [Auth VLAN | Access VLAN] if the device is certified, but not in the Out-of-Band user list** option as described in Add Port Profile, page 3-34.
- If using third party certificates or self-signed certificates for CAS, ensure that the CA certificate is installed in the root store for every Windows domain user. This is important for OOB Logoff to work in a multi-user environment while logging out from Windows.

  In Internet Explorer, click **Tools > Internet Options**. Go to the **Content** tab and click **Certificates.** Go to the **Trusted Root Certificate Authorities** tab and check whether the CA certificate is installed.

Note It is not recommended to use self-signed certificates for enterprise deployment.

Network Requirements

- While using self-signed certificates for CAS, ensure that the certificates are installed in the certificate root store of the client machine.
- In Layer 3 Out-of-Band Real-IP Gateway mode using Virtual Routing and Forwarding (VRF), Policy Based Routing (PBR), or Access Control Lists (ACLs) on the network, Cisco recommends that the CAS certificate should use the untrusted IP or FQDN of the CAS.

- In Layer 3 network topology, when users are moving from one location to another using same CAS name as the Discovery Host, it is recommended to use DNS to resolve the name to the IP of the CAS that is closest to the user.
- Once a device is connected to the Access network, the OOB Logoff heartbeat packets of the NAC Agent must be sent to the same CAS that authenticated the device.

Feature Dependencies - Optional

- In order to enforce OOB Heartbeat Timer, you *must* enable Out-of-Band Logoff. See Configure OOB Heartbeat Timer (per User Role), page 8-18 for more information.
- The Certified Devices List (CDL) is cleared by Out-of-Band Logoff only when the **Require users to be certified at every web login option** in the **CAM Device Management > Clean Access > General Setup > Web Login** web console page is enabled for the user role and appropriate OS. See Web Login, page 1-11 for more details.
- To enable logout of the NAC Agent per role basis when a user logs off the Windows domain, ensure that the **Logoff NAC Agent users from network on their machine logoff or shutdown after <x> secs** option in the **CAM Device Management > Clean Access > General Setup > Agent Login** web console page has been enabled for the user role. See Agent Login, page 1-7 for more details. By default, when **Logout** or **Exit** options are selected from the Cisco NAC Agent icon in the system tray, the Agent sends a logout request to CAS.

Feature Limitations

- Release 4.7(x) and earlier versions of the Cisco NAC Agent and Mac OS X Agent do not support the Out-of-Band Logoff feature.
- User will be logged off if DHCP Renew provides a different IP, or if the client machine moves to second Access VLAN.
- While using Out-of-Band Logoff in a multi-home environment, the NAC agent can track only one login at a time (PRA, Heartbeat, or Logout).

  For example, if a user logs in to the NAC agent through the wireless connection, and then connects the PC and login through the wired connection. At this point, the agent uses only the wired IP address for communication. If the user logs out at this point, the entry using IP from wired connection will be removed from the OUL, but the wireless entry will remain in the OUL. After the OOB Heartbeat Timer expires, the wireless entry will be removed from the OUL. It is recommended to set a short OOB Heartbeat interval to remove the wireless side user appropriately.
- The following failure scenarios might cause the Cisco NAC Agent to appear following successful user authentication when the client machine roams between CASs in Layer 3 (both In-Band and Out-of-Band) and Layer 2 /Layer 3 Out-of-Band environments. Erroneous Agent login dialogs could also appear if users roam from the Cisco NAC Appliance network in Layer 3 mode to a non-NAC network:
  - ARP poisoning
  - Temporary loss of network connection between the client machine and the CAS
  - Access to untrusted interface IP address on the CAS from non-NAC network segments on NAC-enabled client machines

  Cisco offers the following recommendations to prevent this situation:
  - Ensure all trusted networks (post-authentication) can reach the CAS untrusted interface IP address through the CAS trusted interface only

- Block discovery packets from all non-NAC networks to the CAS untrusted interface IP address (discovery packets that arrive on the trusted interface of the CAS are blocked by default)

Note These scenarios are not specific to OOB logoff feature and represent general Cisco NAC Agent behavior for some Out-of-Band topologies.

Enable Out-of-Band Logoff

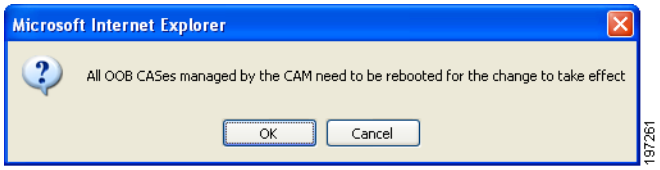
The following steps explain how to enable Out-of-Band Logoff for the NAC and Mac OS X Agents.

Step 1 Go to **Device Management > Clean Access > General Setup > Agent Login** (Figure 9-1).

Step 2 Check the **Enable OOB logoff for Windows NAC Agent and Mac OS X Agent** checkbox. Once enabled, this setting applies to all Out-of-Band CASs managed by this CAM in the Cisco NAC Appliance deployment, applies to all the user roles, and applies to all client machines logging in via the Cisco NAC Agent and Mac OS X Agent, regardless of other settings in assigned user roles.

Step 3 Click **Update** and confirm the requirement to reboot all Out-of-Band CASs associated with this CAM by clicking **OK** in the dialog box that appears (Figure 9-4). After you enable the Out-of-Band logoff feature, full Out-of-Band Logoff functions are not available to Agents logging into the network until you reboot the Out-of-Band CAS. In addition, if you enable Out-of-Band Logoff on one CAS in an HA deployment, you must reboot the CAS-pair if they are already managed by CAM. See Reboot the Clean Access Server, page 2-8.

Figure 9-4 Enable OOB Logoff—Acknowledge Requirement to Reboot CASs


Microsoft Internet Explorer
All OOB CASes managed by the CAM need to be rebooted for the change to take effect
OK
Cancel
197261

Tip To verify whether or not the Out-of-Band Logoff feature is enabled on a particular Out-of-Band CAS, log in to the CAS CLI and enter the **netstat -unl | egrep -w '890[12]'** commands to see if the required ports are open. If so, the CAS should return the following:

```
[root@CAS1]# netstat -unl | egrep -w '890[12]'
udp   0   0 10.0.0.100:8901   0.0.0.0:*
udp   0   0 10.0.0.100:8902   0.0.0.0:*
```

This can be a very useful tool to help quickly determine which Out-of-Band CASs in a multiple-CAS environment do and do not currently have the Out-of-Band Logoff feature enabled.

Troubleshooting OOB Logoff

If you have problems with the OOB Logoff feature, check the following:

- Check whether the client machine is able to reach CAS using the name/IP address after successful login to Access VLAN. This will update the client IP address in Access VLAN in the CAM web console.
- If using the name to reach the CAS, perform a DNS Lookup of the CAS using its Fully Qualified domain name (FQDN).
- Open up wireshark minimally to see if CAS is responding back to Agent logout request.
- Check whether the CAS was rebooted after enabling OOB Logout feature in CAM web console.
- Check the CAS log files by using the following commands:

```
/perfigo/access/tomcat/logs/nac_server.log
/perfigo/access/tomcat/logs/catalina.out
/perfigo/access/apache/logs/access_log
```

- Check the CAM log files by using the following commands:

```
/perfigo/control/tomcat/logs/nac_manager.log
/perfigo/control/tomcat/logs/catalina.out
```

- Check the Event Logs in the CAM web console by clicking **Monitoring > Event Logs > View Logs**.

Note See Cisco NAC Appliance Log Files, page 13-11 for more details.

- Collect the NAC Agent support logs by clicking **Start > All Programs > Cisco > Client Utilities > Cisco Log Packager.**

Configure Restricted Network Access for Agent Users

Administrators can configure restricted network access to users when they choose not to download and install the Cisco NAC Agent or launch the Cisco NAC Web Agent themselves, due to lack of permissions on the machine or for guest access purposes, for example. This enhancement is intended to aid guests or partners in a corporate environment to get access to the network even if their assigned user role requires them to log in via an Agent.

Users can also take advantage of "restricted" network access to gain limited network access when the client machine fails remediation and the user must implement updates to meet network access requirements before they can log in using their assigned user role.

The restricted network access option can only be configured when the **Require use of Agent** and/or **Require use of Cisco NAC Web Agent** checkboxes are enabled, and the option in question allows you to configure the user role to which these users will be assigned in addition to the button and text presented. When the user performs initial web login and is redirected to download the Agent, the "**Restricted Network Access**" text and button will appear below the "**Download Cisco NAC Agent**" and/or "**Launch Cisco NAC Web Agent**" buttons on the page (Figure 9-2 and Figure 9-3) if the "**Allow restricted network access in case user cannot use NAC Agent or Cisco NAC Web Agent**" option is enabled under **Device Management > Clean Access > General Setup | Agent Login**. If the user chooses not to download the Agent or launch the Cisco NAC Web Agent, the user can click "**Get Restricted Network Access**" button to gain the access permitted by the assigned role through the same browser page.

To support Agent login and/or remediation, users can choose to accept "restricted" network access during Agent login dialog sessions when it is clear that the client machine requires update in order to meet network security requirements. During the Agent session, the user can click **Get Restricted Network Access** in the Cisco NAC Agent/Cisco NAC Web Agent dialogs and immediately access the

network using the role you assign for restricted network access, regardless of their assigned user role. For more information, see Windows Cisco NAC Agent User Dialogs, page 10-3 and Cisco NAC Web Agent User Dialogs, page 10-28.

Note that:

- Restricted network access users appear on the In-Band Online Users list denoted by blue shading.

  For example, if a user cannot install the Agent and clicks the "Restricted Access" button in an OOB deployment, that user appears on the In-Band Online User list and remains in the Authentication VLAN even though the CAS is performing OOB. In this case, administrators can configure ACLs on the restricted role to control access for users in that role.
- Restricted network access users do not appear on the Certified Devices List (since they have not met posture assessment requirements).

Configure Network Policy Page (Acceptable Use Policy) for Agent Users

This section describes how to configure user access to a Network Policy page (or Acceptable Usage Policy, AUP) for Agent users. After login and requirement assessment, the Agent displays an "Accept" dialog (Figure 10-53 on page 10-41) with a **Network Usage Terms & Conditions** link to the web page that users must accept to access the network. You can use this option to provide a policies or information page about acceptable network usage. This page can be hosted on an external web server or on the CAM itself.

To Configure Network Policy Link

1. Go to **Device Management > Clean Access > General Setup** (see Figure 9-1 on page 9-4).
2. Make sure **User Role**, **Operating System** and **Require use of Agent/Require Use of Cisco NAC Web Agent** are configured.
3. Click **Show Network Policy to NAC Agent and Cisco NAC Web Agent users [Network Policy Link:]**. This will display a link in the Agent to a Network Usage Policy web page that Agent users must accept to access the network.
4. If hosting the page on the CAM, you will need to upload the page (for example, "helppage.htm") using **Administration > User Pages > File Upload**. See Upload a Resource File, page 5-13 for details. If hosting the page on an external web server, continue to the next step.
5. Type the URL for your network policy page in the **Network Policy Link** field as follows:
   - To link to an externally-hosted page, type the URL in the format:
     `https://mysite.com/helppages`.
   - To point to a page you have uploaded to the CAM, for example, "helppage.htm," type the URL as follows:
     `https://<CAS_IP_address>/auth/helppage.htm`
6. Make sure to add traffic policies to the Temporary role to allow users HTTP access to the page. See Adding Traffic Policies for Default Roles, page 8-27 for details.

To see how the Network Policy dialog appears to Agent users, see Figure 10-53 on page 10-41.

Configure the Agent Temporary Role

See Configure Agent Temporary Role, page 8-19 for details on configuring traffic policies and session timeout for the Agent Temporary role.

Retrieving Cisco NAC Appliance Updates

A variety of updates are available from the Clean Access **Updates** server, available under **Device Management > Clean Access > Updates**. You can perform updates manually as desired or schedule them to be performed automatically. This section describes how to do the following:

- View Current Updates
- Configure and Download Updates
- Configure Proxy Settings for CAM Updates (Optional)

View Current Updates

Step 1 Choose **Device Management > Clean Access > Updates**. The **Summary** page appears by default.

Step 2 The **Current Versions of Updates** section lists all the latest Cisco Updates versions currently on your CAM:

Cisco Checks and Rules

Cisco provides a variety of pre-configured rules ("pr_") and checks ("pc_") for standard client checks such as hotfixes, Windows update, and various antivirus software packages. Cisco checks and rules are a convenient starting point if you need to manually create your own custom checks and rules.

Supported AV/AS Product List (Windows/Macintosh)

The Cisco NAC Appliance Supported AV/AS Product List is a versioned XML file distributed from a centralized update server that provides the most current matrix of supported antivirus (AV) and antispyware (AS) vendors and product versions used to configure AV or AS Rules and AV or AS Definition Update requirements for posture assessment/remediation. This list is updated regularly for the AV/AS products and versions supported in each Agent release and to include new products for new Agent versions. Note that the list provides version information only. When the CAM downloads the Supported AV/AS Product List it is downloading the information about what the latest versions are for AV/AS products; it is not downloading actual patch files or virus definition files. Based on this information, the Agent can then trigger the native AV/AS application to perform updates.

Having the latest Supported AV/AS list ensures your AV/AS rule configuration pages include all the new products supported in the new Agent, particularly if you have updated the Agent version on your CAM.

For the latest details on products and versions supported, see **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**, or see the "Clean Access Supported AV/AS Product List" section in the latest Release Notes.

Default Host Policies

Clean Access provides automatic updates for the default host-based policies (for Unauthenticated, Temporary, and Quarantine roles). Note that Default Allowed Hosts are disabled by default, and must be enabled for each role under **User Management > User Roles > Traffic Control > Hosts**. See Enable Default Allowed Hosts, page 8-9 for details.

Default L2 Policies

Displays the current version of Default Layer 2 traffic policies available on the CAM. Whenever the CAM searches for updates (either manually or automatically using the settings in the **Device Management > Clean Access > Updates** page), it automatically checks to see if there is a newer version of Default Layer 2 traffic policies available.

OS Detection Fingerprint:

By default, the system uses the User-Agent string from the HTTP header to determine the client OS. In addition, platform information from JavaScript or the OS fingerprinting from the TCP/IP handshake can also be compared against the OS signature information in the CAM database to determine the client OS. This information can be updated in the CAM when new OS signatures become available in order to verify an OS fingerprint as a Windows machine. This enhanced OS fingerprinting feature is intended to prevent users from changing identification of their client operating systems through manipulating HTTP information. Note that this is a "passive" detection technique (accomplished without Nessus) that only inspects the TCP handshake and is not impacted by the presence of a personal firewall. See also **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > OS Detection** in the CAS management pages of the web console, and the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for further details.

Note The OS detection/fingerprinting feature uses both browser User-Agent string and TCP/IP stack information to try to determine the OS of the client machine. While the detection routines will attempt to find the best match, it is possible that the OS may be detected incorrectly if the end-user modifies the TCP/IP stack on the client machine and changes the User-Agent string on the browser. If there is concern regarding malicious users evading the OS fingerprinting/detection mechanisms, then administrators are advised to use network scanning in order to confirm the OS on the machine. If, for any reason, it is not possible or not desirable to use network scanning, then network administrators should consider pre-installing the Agent on client machines or allowing users to log in via the Cisco NAC Web Agent.

In a FIPS 140-2 compliant network where both the CAMs and CASs are configured in failover mode, Cisco NAC Appliance does not correctly report the operating system of a client machine following a failover event and subsequent synchronization. Once the CAM/CAS detect client HTTP/HTTPS traffic, the CAM/CAS are able to "rediscover" the client machine operating system following the failover event.

Windows NAC Agent

Displays the current version of the Cisco NAC Windows Agent installed on the CAM. This is the version of Cisco NAC Agent that users upload and install on their client machines when they first sign in to Cisco NAC Appliance.

Compliance Module for Windows

Displays the current version of the AV/AS vendor application support package available to Windows client machines logging into the Cisco NAC Appliance system.

Macintosh Clean Access Agent

Displays the current version of the Mac OS X Cisco NAC Agent available on the CAM. This is the version of Mac OS X Agent that users upload and install on their client machines when they first sign in to Cisco NAC Appliance. The Mac OS X Agent is automatically updated to a more current version when users sign in and a newer version of the Agent is available on the CAM.

Compliance Module for Mac

Displays the current version of the AV/AS vendor application support package available to Macintosh client machines logging into the Cisco NAC Appliance system.

Cisco NAC Web Agent

Displays the current version of the Cisco NAC Web Agent currently installed on the CAM. Users who log in and choose to use the temporal Cisco NAC Web Agent always receive the current version of the Agent for their user session.

Cisco NAC Web Agent Facilitator (ActiveX/Applet)

Displays the current version of the Cisco NAC Web Agent ActiveX/Java Applet the CAM uses to install the temporal Agent on the client machine when users access Cisco NAC Appliance and choose to use the Cisco NAC Web Agent.

L3 MAC Address Detection (ActiveX/Applet

The L3 Java Applet and L3 ActiveX web client are needed for client MAC Address detection when users perform web login in L3 OOB deployments. The MAC detection mechanism of the Agent will automatically acquire the client MAC address in L3 OOB deployments. (See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for more information.)

Users performing web login will download and execute either an ActiveX control (for IE browsers) or Java applet (for non-IE browsers) to the client machine prior to user login to determine the user machine's MAC address. This information is then reported to the CAS and the CAM to provide the IP address/ MAC address mapping.

ActiveX/Java Applet and Browser Compatibility

- Complete ActiveX/Java Applet and Browser Compatibility information is available in *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.
- Due to Firefox issues with Java, Java applets are not supported for Firefox on Mac OS X. See the Firefox release notes (http://www.mozilla.com/firefox/releases/1.5.0.3.html) for details.

Note

- To ensure Clean Access checks include the latest Microsoft Windows hotfixes, always get the latest **Updates** of Cisco Checks and Rules (by Clean Update if needed) and ensure appropriate host-based traffic policies are in place (see Add Global Host-Based Traffic Policies, page 8-8 for details.)
- When upgrading your CAM/CAS to the latest release of Cisco NAC Appliance, all Perfigo/Cisco pre-configured checks/ rules will be automatically updated.

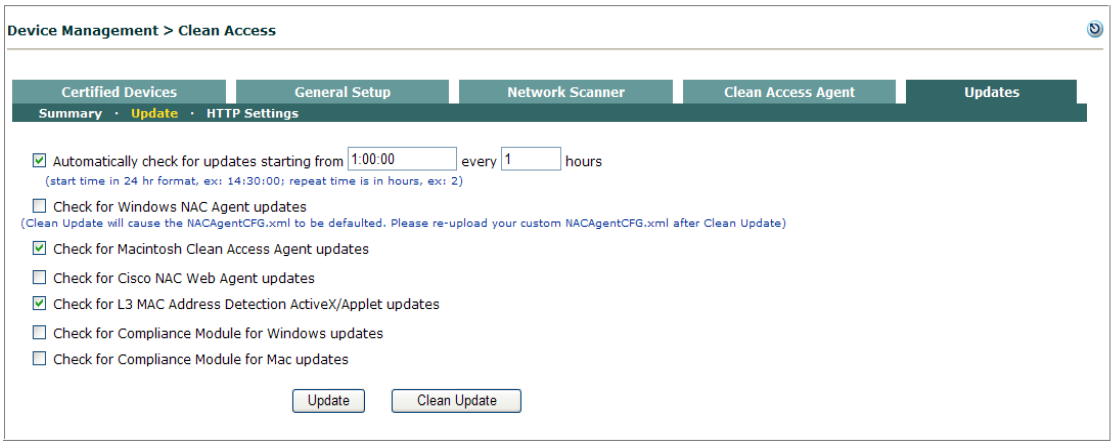
Step 3 Once updates are performed (manual or automatic), you can check the Summary page to verify the updates.

Configure and Download Updates

Step 1 Go to **Device Management > Clean Access > Updates**.

Step 2 Click the **Update** subtab to configure what Cisco Updates to download to your CAM and/or how often to check for Clean Access Updates. (Figure 9-5).

Figure 9-5 Device Management > Clean Access > Updates > Update


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Summary · Update · HTTP Settings
Automatically check for updates starting from 1:00:00 every 1 hours
(start time in 24 hr format, ex: 14:30:00; repeat time is in hours, ex: 2)
Check for Windows NAC Agent updates
(Clean Update will cause the NACAgentCFG.xml to be defaulted. Please re-upload your custom NACAgentCFG.xml after Clean Update)
Check for Macintosh Clean Access Agent updates
Check for Cisco NAC Web Agent updates
Check for L3 MAC Address Detection ActiveX/Applet updates
Check for Compliance Module for Windows updates
Check for Compliance Module for Mac updates
Update
Clean Update
303219

Step 3 To configure automatic updates on your CAM, click the checkbox for **Automatically check for updates starting from [] every [] hours**, type a start time in 24-hour format (such as 13:00:00), and type a "repeat" interval (**1** hour is recommended).

Step 4 Click the **Check for Windows NAC Agent updates** option to ensure the CAM always downloads the latest version of the Agent installer. This must be enabled for Agent auto-upgrade.

Step 5 Click the **Check for Macintosh Clean Access Agent updates** option to ensure the CAM always downloads the latest version of the Agent. This must be enabled for Macintosh Clean Access Agent auto-upgrade.

Step 6 Click the **Check for Cisco NAC Web Agent updates** option to ensure the CAM always downloads the latest version of the Cisco NAC Web Agent.

Step 7 Click the **Check for L3 MAC Address Detection ActiveX/Applet updates** option to ensure the CAM always downloads the latest versions of the L3 Java Applet and ActiveX web clients. Web login users need to download these helper controls from the login page to enable the CAS to obtain MAC information in L3 deployments (particularly for L3 OOB). Once the Agent is used, the Agent automatically sends client MAC information to the CAS.

Step 8 Click the **Check for Compliance Module for Windows Updates** option to automatically poll the update repository for the latest version of the AV/AS vendor support package that you can make available to Windows client machines during their next login session. For more information on enabling updated AV/AS posture pack downloads to client machines, see Agent Distribution, page 9-18.

Step 9 Click the **Check for Compliance Module for Mac Updates** option to automatically poll the update repository for the latest version of the AV/AS vendor support package that you can make available to Macintosh client machines during their next login session. For more information on enabling updated AV/AS posture pack downloads to client machines, see Agent Distribution, page 9-18.

Step 10 Do one of the following:

a. Click **Update** to manually update your existing database with the latest Cisco checks and rules, Agent update, Supported AV/AS Product List, and default host policies.

b. Click **Clean Update** to remove previous update items from the database first (including non-customer-created checks and rules, Agent updates, and Supported AV/AS Product Lists) before downloading the new updates. See Enable Default Allowed Hosts, page 8-9 for details.

Step 11 When you retrieve updates, the following status messages are displayed at the bottom of the page:

- **Cisco auto-update schedule** (if enabled)
- **Latest version of Windows NAC Agent Installer** (if available)
- **Latest version of Macintosh Clean Access Agent Installer** (if available)
- **Latest version of the Compliance Module update for Windows**
- **Latest version of Cisco Checks & Rules:**
  This shows the version of Cisco checks and rules downloaded. The latest update of Cisco pre-configured checks ("**pc_**") and rules ("**pr_**") will populate the **Check List** and **Rule List**, respectively (under **Device Management > Clean Access > Clean Access Agent > Rules**).
- **Latest Cisco NAC Web Agent version**, **Cisco NAC Web Agent Applet Facilitator version**, and **Cisco NAC Web Agent ActiveX Facilitator version** installed
- **Latest version of Supported AV/AS Product List:**
  This shows the latest version of the Supported AV/AS Product List. When creating a **New AV Rule** or requirement of type **AV Definition Update,** the matrix of supported vendors and product versions will be updated accordingly.
- **Latest version of default host policies:**
  This shows the latest version of default host-based policies provided for the Unauthenticated, Temporary, and Quarantine roles.
- **Latest version of OS detection fingerprint**:
  Updates to OS Detection Fingerprints (or signatures) will be made as new operating systems become available for Windows machines.
- **Latest version of L3 Java Applet web client**:
  Updates to the L3 Java Applet web client will be downloaded and published as they are made available.
- **Latest version of L3 ActiveX web client**:
  Updates to the L3ActiveX web client will be downloaded and published as they are made available.
- **Latest version of OOB switch OIDs**:
  Updates to the object IDs (OIDs) of supported switches will be downloaded and published as they are made available.



Note Starting from Release 4.5, administrators are able to update the object IDs (OIDs) of supported WLC platforms (in addition to supported switches) when performing a CAM update.

- **Latest version of default L2 policies**:
  Updates to the Layer 2 traffic policies are downloaded and published as they are made available.

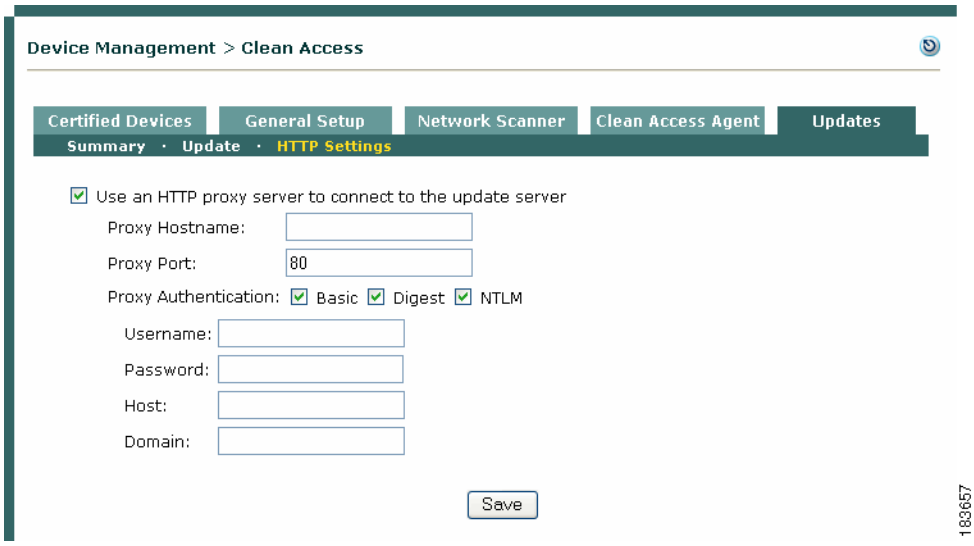
Configure Proxy Settings for CAM Updates (Optional)

If your CAM requires a proxy server to connect to the Internet, configure proxy server settings so that r the CAM can get Clean Access Updates.

Step 1 Go to **Device Management > Clean Access > Updates**.

Step 2 Click the **HTTP Settings** subtab.

Figure 9-6 Device Management > Clean Access > Updates > HTTP Settings



Step 3 Click the "**Use an HTTP proxy server to connect to the update server**" option if your CAM goes through a proxy server to get to the Internet.

Step 4 Specify the **Proxy Hostname** and **Proxy Port** the CAM uses to connect to the Internet.

Step 5 If your proxy server requires credentials to authenticate the proxy session, specify the **Proxy Authentication** method by checking one or more of the following:

- **Basic**—Prompts you to provide the **Username** and **Password** required to authenticate the proxy session between the CAM and the proxy server.
- **Digest**—Just as with the **Basic** setting, this option prompts you to provide the **Username** and **Password** required to authenticate the proxy session between the CAM and the proxy server and provides the additional bonus of "hashing" the credentials and requiring the proxy service to digest the information in order to keep the username and password protected across networks.
- **NTLM**—In addition to the **Username** and **Password** required to authenticate the proxy session between the CAM and the proxy server, you must also specify the proxy **Host** and **Domain** to support an existing Microsoft Windows NT LAN Manager (NTLM) proxy service.

Note The **NTLM** option supports NTLM Version 1 and Version 2.

Step 6 Click **Save**.

Setting Up Agent Distribution/Installation

The latest version of the Agent is automatically included with the Clean Access Manager software for each software release. The CAM automatically publishes the Agent installation file to each Clean Access Server after CAS installation and anytime the CAM acquires a new version of the Agent through web Updates or through a manual upload.

To enable users to download and install the Agent installation file or launch the Cisco NAC Web Agent, you must Require Agent Login for Client Machines, page 9-3. For new Agent users, the Agent download page appears after the user logs in for the first time via the web login. If auto-upgrade is enabled, existing Agent users are prompted at login to upgrade if a new Agent version becomes available. Cisco NAC Web Agent users connect to the network automatically as long as the client machine complies with configured network security parameters.

Note Users without administrator privileges upgrading their Windows client machine from an earlier version of the Clean Access Agent (version 4.5.2.0 or 4.1.10.0 and earlier) to the Cisco NAC Agent must have the **CCAAgentStub.exe** Agent Stub installed on the client machine to facilitate upgrade. (Users with administrator privileges do not need this file.) After successful Cisco NAC Agent installation, the user is not required to have administrator privileges on the client machine, nor is the **CCAAgentStub.exe** Agent Stub file needed. For more information on the **CCAAgentStub.exe** file, see the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

This section describes the following:

- Agent Distribution, page 9-18
- Installation Page, page 9-20
- Cisco NAC Agent XML Configuration File Settings, page 9-23
- Agent Customization File Settings, page 9-33
- Cisco NAC Agent MSI Installer, page 9-37

Agent Distribution

The Distribution page provides the following configuration options pertinent to the Agent.

- **NAC Agent Temporary Role**—Displays the name of the Agent temporary role (default is "Temporary"). To change the Role Name, see Editing an Existing Role, page 6-14.

Note

- The **Enable L3 support** option must be checked on the CAS (under **Device Management > Clean Access Servers > Manage [CAS_IP] > Network > IP**) for the Agent to work in VPN tunnel mode. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for additional information.
- VPN Clients must be in L3 deployment and should not be in the managed subnet or the management interface subnet of CAS.

- **Windows NAC Agent Current Version**—The version of the Windows Agent installation file to be downloaded by the client machine. The upgrade version reflects what the CAM has downloaded from the Updates page. See Require Agent Login for Client Machines, page 9-3.

Note Users without administrator privileges upgrading their Windows client machine from an earlier version of the Clean Access Agent (version 4.5.2.0 or 4.1.10.0 and earlier) to the Cisco NAC Agent must have the **CCAAgentStub.exe** Agent Stub installed on the client machine to facilitate upgrade. (Users with administrator privileges do not need this file.) After successful Cisco NAC Agent installation, the user is not required to have administrator privileges on the client machine, nor is the **CCAAgentStub.exe**

Agent Stub file needed. or more information on the **CCAAgentStub.exe** file, see the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

- **Mac Clean Access Agent Current Version**—The version for the Macintosh Clean Access Agent installation file. The upgrade version reflects what the CAM has downloaded from the Updates page. See Require Agent Login for Client Machines, page 9-3.
- **Windows Compliance Module** —The current version of the AV/AS vendor support package available to client machines. When client machines log into Cisco NAC Appliance via the Cisco NAC Agent and check to see whether or not a new version of the Agent is available, the discovery process also helps determine whether or not the AV/AS support information on the client is up-to-date. If it is not, then the client may get the updated package, depending on whether or not you have enabled the **Current Compliance Module is a mandatory upgrade** option and, if not, whether the user chooses to update their AV/AS support package at that moment.
- **Mac Compliance Module** —The current version of the AV/AS vendor support package available to client machines. When client machines log into Cisco NAC Appliance via the Mac OS X Agent and check to see whether or not a new version of the Agent is available, the discovery process also helps determine whether or not the AV/AS support information on the client is up-to-date. If it is not, then the client may get the updated package, depending on whether or not you have enabled the **Current Compliance Module is a mandatory upgrade** option and, if not, whether the user chooses to update their AV/AS support package at that moment.
- **Current NAC Agent is a mandatory upgrade**—Checking this option and clicking **Update** forces the user to accept the prompt to upgrade to the latest version of the Agent when attempting login. If left unchecked (optional upgrade), the user is prompted to upgrade to the latest Agent version but can postpone the upgrade and still log in with the existing Agent. See Disable Mandatory Agent Auto-Upgrade on the CAM, page 9-103.

Note New CAM/CAS installs automatically set the **Current NAC Agent is a mandatory upgrade** option by default under **Device Management > Clean Access > Clean Access Agent > Distribution**. For CAM/CAS upgrades, the current setting (enabled or disabled) will be carried over to the upgraded system.

The **Current NAC Agent is a mandatory upgrade** option only applies to Windows Agents for release 4.1(2) and earlier.

- **Do not offer current NAC Agent to users for upgrade**—Checking this option and clicking **Update** prevents upgrade notifications (mandatory or optional) to all Agent users, even when an Agent update is available on the CAM.
- **Current Compliance Module is a mandatory upgrade**—Enabling this option forces client machines logging in via the Cisco NAC Windows Agent to update their AV/AS vendor support package when the current version on the client machine is not up-to-date. The user is prompted to update the AV/AS vendor support package.
- **Do not offer current Compliance Module to users for upgrade**—This option gives you the ability to withhold the most recent AV/AS vendor update package from users logging into the Cisco NAC Appliance system via the Cisco NAC Windows Agent. (You may want to enable this feature if you need to test the level of support for one or more vendor applications in the latest package to ensure they are appropriate for users accessing your network before making the AV/AS support package update available to users.)

- **Allow downgrade of Compliance Module**—Checking this option enables you to provide an earlier version of the AV/AS support package for users logging in via the Cisco NAC Windows Agent. When the Agent performs discovery with the Cisco NAC Appliance system to start the next user login session, if the **Allow downgrade of Compliance Module** option is enabled, the Agent automatically gets the "downgraded" AV/AS support package from the CAS regardless of the current version of the AV/AS support package currently on the client machine.
- **Upload Agent/Compliance Module File**—Use the **Browse** button and navigate to the folder where the appropriate Agent file is located. Select the Agent file, enter a version number in the **Agent Version** field, and click **Upload** to manually upload the Cisco NAC Agent installation file (nacagentsetup-win.tar.gz) or AV/AS Posture pack (**av-posture-pack-win.tar.gz** or **av-posture-pack-mac.tar.gz**) in this field. You can leave the **Agent Version** field empty for compliance module.

  For details on uploading Windows and Macintosh versions of the earlier Clean Access Agent, refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

Note The CAM does not accommodate Cisco NAC Agent installation files (nacagentsetup-win.tar.gz) and Windows Clean Access Agent Setup files (CCAAgentSetup-4.x.y.z.tar.gz) simultaneously. If you upload an older Windows Clean Access Agent Setup file, you will wipe out the existing Cisco NAC Agent installation and XML Agent configuration files, and vice-versa.

Note Starting from release 4.6(1), the CAM no longer manages Clean Access Agent Patch/Upgrade files (CCAAgentUpgrade-4.x.y.z.tar.gz). Be sure you only upload Clean Access Agent installation files (CCAAgentSetup-4.x.y.z.tar.gz or CCAAgentMacOSX-4.x.y.z-k9.tar.gz) from the Cisco Software Download Site.

Caution You must upload the Agent file as a **tar.gz** file (without untarring it) to the CAM. Make sure you do NOT extract the .exe file before uploading.

See also Manually Uploading the Agent to the CAM, page 9-100.

- **Version**—For manual upload, keep the same version number used for the Agent when downloading.

Installation Page

You can configure the level of user interaction needed when the Agent is initially installed.

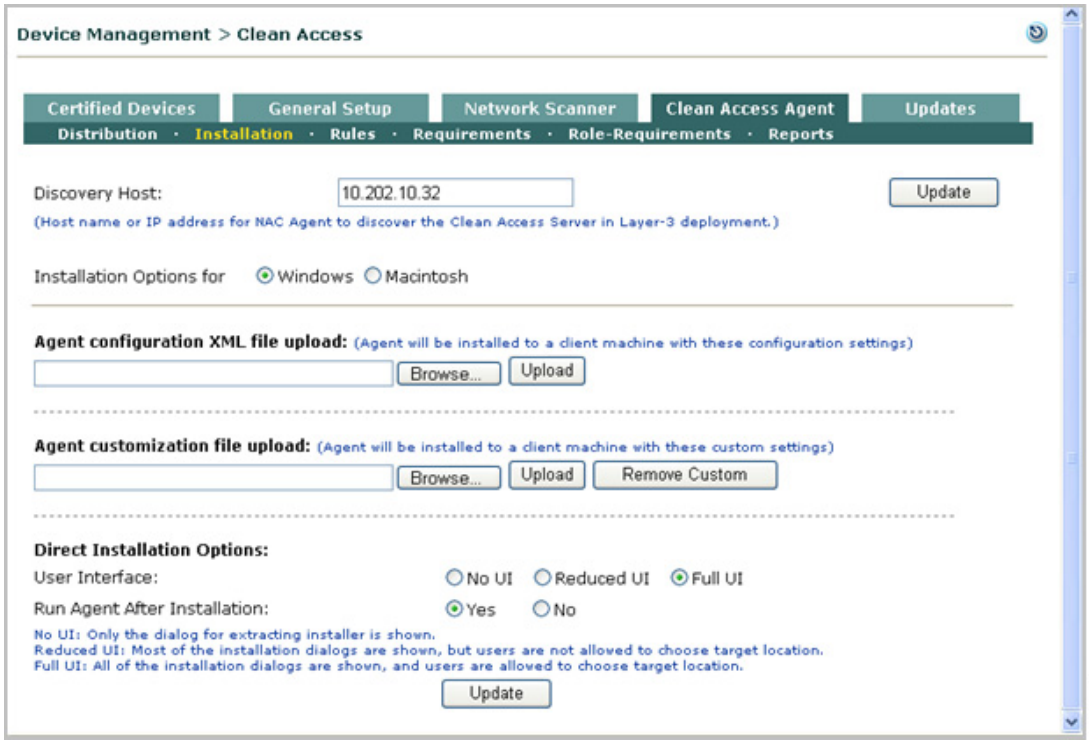
Note Once one of the persistent Agents is installed, Agent launch and uninstallation shortcuts appear on the desktop.

To configure installation options:

Step 1 Make sure use of the Agent is required as described in Require Agent Login for Client Machines, page 9-3.

Step 2 Go to **Device Management > Clean Access > Clean Access Agent > Installation**.

Figure 9-7 Agent Installation Page


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Distribution · Installation · Rules · Requirements · Role-Requirements · Reports
Discovery Host:
10.202.10.32
Update
(Host name or IP address for NAC Agent to discover the Clean Access Server in Layer-3 deployment.)
Installation Options for
Windows
Macintosh
Agent configuration XML file upload: (Agent will be installed to a client machine with these configuration settings)
Browse...
Upload
Agent customization file upload: (Agent will be installed to a client machine with these custom settings)
Browse...
Upload
Remove Custom
Direct Installation Options:
User Interface:
No UI
Reduced UI
Full UI
Run Agent After Installation:
Yes
No
No UI: Only the dialog for extracting installer is shown.
Reduced UI: Most of the installation dialogs are shown, but users are not allowed to choose target location.
Full UI: All of the installation dialogs are shown, and users are allowed to choose target location.
Update
278629

- **Discovery Host**—This field is used by the Agent to send a proprietary, encrypted, UDP-based protocol to the Clean Access Manager to discover the Clean Access Server in Layer 3 deployment. The field automatically populates with the CAM's IP address (or DNS host name). In most cases, the default IP address does not need to be changed, but in cases where the CAM's IP address is not routed through the CAS, the Discovery Host can be any IP address or host name that can be reached from client machines via the CAS. Upon initial installation or when a new Agent configuration XML file is passed to the client machine via the CAS, the Cisco NAC Agent automatically uses this value for the DiscoveryHost parameter in the Agent configuration XML file, which is required to perform successful Agent login.

Note When the Discovery Host value is changed, it is received only by the new Agents that are deployed. The existing Agents do not receive the changed IP address. You need to use the "overwrite" function in the DiscoveryHost parameter in the Agent configuration XML file, for the existing Agents to receive the changed Discovery Host value. Refer to Table 9-4 on page 9-27 for more information.

Note The Discovery Host is set to the IP of the CAM by default because the CAM must always be on a routed interface on the trusted side of the CAS. This means any client traffic on the untrusted side must pass through a CAS in order to reach the IP of the CAM. When the client attempts to contact the Discovery Host IP, the CAS will intercept the traffic and start the login process. It is assumed that best practices are applied to protect the CAM with ACLs, and that no client traffic should ever actually arrive at the CAM. For extra security (once L3 is correctly deployed), you can change the Discovery Host to an IP other than the CAM IP on the trusted side.

Step 3 The **Installation Options** are enabled by default for **Windows**.

Step 4 Use the **Agent configuration XML file upload** option if you want to customize login and session behavior on Windows client machines with the Cisco NAC Agent installed:

a. Create an Agent configuration XML file entitled **NACAgentCFG.xml** and ensure you have saved it on a local machine. For an example XML file template and a complete list of parameters and available settings, see Cisco NAC Agent XML Configuration File Settings, page 9-23.

b. Click **Browse** and navigate to the directory on your local machine where the **NACAgentCFG.xml** Agent configuration file resides, highlight it in the dialog box, and click **Upload**.

The next time the user authenticates with Cisco NAC Appliance, or if you enforce a mandatory update for the Cisco NAC Agent, the new Agent configuration is automatically enabled on the client machine.

Step 5 Use the **Agent customization file upload** option to customize the NAC Agent UI on Windows client machines with Cisco NAC Agent that is compatible with the CAM Release installed.

Note The **Agent customization file upload** option is not available for Cisco NAC Agent earlier than version 4.8.0.32.

a. Create an Agent customization file and save the file on a local machine. For the available settings, see Agent Customization File Settings, page 9-33.

b. Click **Browse** and navigate to the directory on your local machine where the Agent customization file resides, select the file, and click **Upload**.

The next time the user performs a fresh install or upgrades the Cisco NAC Agent, the new Agent customization is enabled on the client machine.

Note Click **Remove Custom** to remove the Agent Customization. The next time the user performs a fresh install or upgrades the Cisco NAC Agent, the customization is removed from the client machine.

Step 6 When the installer is launched directly by the user on the machine, choose from the following **Direct Installation Options**:

- **User Interface**:

  No UI—After the user clicks **Open** in the File Download dialog for the Cisco NAC Agent installation file (nacagentsetup-win.tar.gz), there is no user input required. The “Preparing to Install” dialog only appears briefly and the Agent is downloaded and installed automatically.

  Reduced UI—After the user clicks **Open to launch** (or Saves and executes) the Cisco NAC Agent installation file (nacagentsetup-win.tar.gz), the “Preparing to Install” and InstallShield Wizard “Installing Cisco NAC Agent” screens display, but user input fields (such as “Next” buttons) are disabled, and the Agent is extracted and installed automatically.

  Full UI (default)—After the user clicks **Open** (or Saves and executes) the Cisco NAC Agent installation file (nacagentsetup-win.tar.gz), the normal installation dialogs appear. The InstallShield Wizard for the Agent displays, including the Destination Folder directory screen, and, in the case of the Clean Access Server, the user must click through the panes using the “Next,” “Install,” and “Finish” buttons to complete the installation.

- **Run Agent After Installation**:

  Yes (default)—The Agent Login screen pops up after the Agent is installed.

No—The Agent Login screen does not appear after the Agent is installed. The user must double-click the Agent shortcut on the desktop to start the Agent and display it on the taskbar. The Agent can be verified to be installed under **Control Panel > Add/Remove Programs > Cisco NAC Agent**. Once the Agent is started, the Login screen will pop up if **Pop Up Login Window** is enabled on the taskbar menu.

Step 7 Click **Update** to save settings.

Note For MSI installation instructions pertaining to the Cisco NAC Agent, see Cisco NAC Agent MSI Installer, page 9-37.

Cisco NAC Agent XML Configuration File Settings

This section describes how to configure and enable various Cisco NAC Agent features by specifying settings within the **NACAgentCFG.xml** Agent configuration file. Topics include:

- Customize Cisco NAC Agent Login/Logout Dialog Behavior
- Cisco NAC Agent Posture Assessment Report Display Setting
- Specify the Cisco NAC Agent Log File Size
- Manage the Cisco NAC Agent Discovery Host Address
- Specify Server Rule Names
- Cisco NAC Agent Verifying Launch Program Executable for Trusted Digital Signature
- Additional SWISS Discovery Customization
- HTTP Discovery Customization
- Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs
- Client-Side MAC Address Management
- Enable or Disable Cisco NAC Agent Accessibility Interaction
- Specify Cisco NAC Agent Localization Settings

In order to configure a Windows client machine to use any of these additional features for the Cisco NAC Agent, you must define the appropriate parameters in the Agent configuration XML file, ensure that you title the file **NACAgentCFG.xml**, and upload the file to the CAM so that the next time a client machine installs the Cisco NAC Agent (or if you mandate an update to the Cisco NAC Agent for existing users), the new settings are automatically "pushed" to the Agent installation directory on the client machine. The default install directory on Windows 8.1/8/7/Vista/XP is **C:\Program Files\Cisco\Cisco NAC Agent**. However, you may specify a different directory.

When configuring a customized Agent configuration XML file, the administrator can choose to customize one or more (or all) settings and specify whether they should merge with or overwrite existing XML configuration settings on the client machine. In addition to providing specific values for the parameters defined below, the administrator can use the “mode” attribute in conjunction with the target XML parameter to direct the Agent to “merge” the setting with existing parameters, or simply “overwrite” existing settings.

- **“merge”**—specifies a value for a previously undefined XML setting and is ignored if a specific XML setting already exists on the client machine. This is the default behavior for the XML configuration file download feature.

- **"overwrite"**—the XML setting specified in the Agent configuration XML file automatically takes precedence over any existing value currently on the client machine.

For example, a `<Locale mode="merge">German</Locale>` entry in an Agent configuration XML file instructs the Agent not to change any previously-existing Locale setting on the client machine (merge instead of overwrite), but if no setting currently exists, then make the localization language German. If the example entry reads `<Locale mode="overwrite">German</Locale>`, then the new localized language setting for the Agent is German, regardless of whether or not any previous setting exists.

Note The administrator can deploy a configuration XML without certain parameters and later add them when required. The administrator can upload a new configuration XML file including the parameters. These parameters can be set with either "merge" or "overwrite" mode, as they had never been deployed previously.

If the mode is set to "merge", the parameter is added if it does not exist in the configuration file present the client machine. But, if the administrator has allowed the end user to add a parameter to the configuration file and if the parameter value already exists, the "merge" will fail.

If the administrator wants to overwrite all the values regardless of the parameters added by the end user, then the "overwrite" mode can be used.

For instructions on uploading the Agent configuration file to the CAM for eventual download to Agent machines, see Installation Page, page 9-20. For more information on the Cisco NAC Agent and its capabilities, see Cisco NAC Agent, page 10-1.

Note For information on enabling similar functions on client machines where the Clean Access Agent is installed, refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

To ensure that the Cisco NAC Agent adopts any custom settings you specify in the Agent configuration XML, construct the file as shown in the following XML file example template:

Example Agent Configuration XML File Template:

```
<?xml version="1.0" ?>
<cfg>
    <VlanDetectInterval>0</VlanDetectInterval>
    <RetryDetection>3</RetryDetection>
    <PingArp>0</PingArp>
    <PingMaxTimeout>1</PingMaxTimeout>
    <DisableExit>0</DisableExit>
    <AllowCRLChecks>1</AllowCRLChecks>
    <SignatureCheck>0</SignatureCheck>
    <RememberMe>1</RememberMe>
    <AutoPopUp>1</AutoPopUp>
    <AutoPopUpEnable>1</AutoPopUpEnable>
    <ShowMandatoryScreen>0</ShowMandatoryScreen>
    <PostureReportFilter>displayFailed</PostureReportFilter>
    <BypassSummaryScreen>yes</BypassSummaryScreen>
    <LogFileSize>5</LogFileSize>
    <DiscoveryHost></DiscoveryHost>
    <DiscoveryHostEditable>1</DiscoveryHostEditable>
    <ServerNameRules>host.match.com,*.match.com,*.com</ServerNameRules>
    <Locale>default</Locale>
    <AccessibilityMode>0</AccessibilityMode>
    <SwissTimeout>1</SwissTimeout>
```

```
    <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
    <HttpTimeout>120</HttpTimeout>
    <DisableL3SwissDelay>0</DisableL3SwissDelay>
    <ExceptionMACList></ExceptionMACList>
    <GeneratedMAC></GeneratedMAC>
</cfg>
```

Note If the configuration file consists of any invalid parameter, that parameter will not be updated in the client machines.

Table 9-1 Customize Cisco NAC Agent Login/Logout Dialog Behavior

Parameter	Default Value	Valid Range	Description/Behavior
RememberMe	0	0 or 1	If this setting is any value other than **0**, the user only needs to enter login credentials once. The Cisco NAC Agent also remembers the user credentials after session termination/time-out. **Note** When the user logs out of Windows, the saved credentials are erased. When the user moves from a connection that requires username and password to an SSO session and returns back, then the credentials are removed.
AutoPopUp	1	0 or 1	• If this setting is **1**, the Cisco NAC Agent login dialog appears automatically when the user is logged out. • If this setting is **0**, users must manually initiate login using the Start menu option or the system tray icon on the desktop.
AutoPopUpEnable	1	0 or 1	• If this setting is **1**, the Auto PopUp option is enabled. • If this setting is **0**, the Auto PopUp option is disabled. **Note** When this setting is changed by the user manually, the client machine should be rebooted to enable the configuration change. If the configuration file is pushed to the client from the CAM, then it is automatically enabled.
ShowMandatoryScreen	0	0 or 1	When mandatory upgrade is configured on the CAM, a mandatory upgrade window is displayed in the client machine. • If this setting is **0**, the mandatory upgrade window that pops up in the client is disabled. The upgrade will happen without notifying the user. • If this setting is **1**, the mandatory upgrade window is enabled.

Table 9-1 Customize Cisco NAC Agent Login/Logout Dialog Behavior (continued)

Parameter	Default Value	Valid Range	Description/Behavior
BypassSummaryScreen	yes	yes or no	If you are employing auto-remediation for Cisco NAC Agent requirements, this setting enables you to make the Agent session dialog more "automated" by skipping the Agent posture assessment summary screen and proceeding directly to the first auto-remediation function, thus reducing or eliminating user interaction during the Agent login and remediation session.
DisableExit	0	0 or 1	If this parameter is set to 1, users cannot exit the Cisco NAC Agent via the system tray icon.
AllowCRLChecks	1	0 or 1	Setting this parameter to 0 turns off Certificate Revocation List (CRL) checking for the Cisco NAC Agent during discovery and negotiation with the CAS.

Table 9-2 Cisco NAC Agent Posture Assessment Report Display Setting

Parameter	Default Value	Valid Range	Description/Behavior
PostureReportFilter	**displayFailed**	—	This parameter controls the level/type of results that appear to the user when the client machine undergoes posture assessment. • If this setting is **displayAll**, the client posture assessment report appears, displaying all results when the user clicks **Show Details** in the Cisco NAC Agent dialog. • If this setting is **DisplayFailed**, the client posture assessment report only displays remediation errors when the user clicks **Show Details** in the Cisco NAC Agent dialog.

Table 9-3 Specify the Cisco NAC Agent Log File Size

Parameter	Default Value (Decimal)	Valid Range	Description/Behavior
LogFileSize	5	0 and above	This setting specifies the file size (in Megabytes) for Cisco NAC Agent log files on the client machine. • If this setting is 0, the Agent does not record any login or operation information for the user session on the client machine. • If the administrator specifies any other integer, the Cisco NAC Agent records login and session information up to the number of MB specified.[1]

1. Cisco NAC Agent log files are recorded and stored in the **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco NAC Agent\logs** directory. After the first Agent login session, two files reside in this directory: one backup file from the previous login session, and one new file containing login and operation information from the current session. If the log file for the current Cisco NAC Agent session grows beyond the specified file size, the first segment of Agent login and operation information automatically becomes the "backup" file in the directory and the Agent continues to record the latest entries in the current session file.

Table 9-4 Manage the Cisco NAC Agent Discovery Host Address

Parameter	Default Value	Valid Range	Description/Behavior
DiscoveryHost	—	IP address or FQDN	This setting specifies the Discovery Host address the Agent uses to connect to the Cisco NAC Appliance system in a Layer 3 deployment. You can use this function to "overwrite" or "merge" the existing Discovery Host value specified on the CAM with the value currently on the client machine. **Note** If you choose to "merge" this value, the client machine always assumes the Discovery Host specified on the CAM by default. If you choose to "overwrite" (change) this value on the client machine with one on the CAM, you must first change the Discovery Host value in the **CAM Device Management > Clean Access > Clean Access Agent > Installation** web console page and then specify the same value for this parameter.
DiscoveryHostEditable	1	0 or 1	In the **NACAgentCFG.xml** file, if the parameter for **DiscoveryHostEditable** is set to "1" (the default value), then the user can specify a custom value in the Discovery Host field in the Agent Properties dialog box. You can change this entry to "0" to ensure that the user cannot update the value in the Discovery Host field on the client machine.

Table 9-5 Specify Server Rule Names

Parameter	Default Value	Valid Range	Description/Behavior
ServerNameRules	—	FQDN	This parameter consists of comma separated names of servers. The server names available in this list are used for authorization of CAS by client machine. If this list is empty, then the authorization is not performed. The Agent compares the CN (canonical name) in the certificate provided by the CAS/Agent SSL communication with the ServerNameRules parameters in the **NACAgentCFG.xml** file. The CN contains information like host name and domain name. The Agent pops up only when these names match. The server names should be FQDN names. The parameter can be placed anywhere in the **NACAgentCFG.xml** file. IP Addresses can also be used if they match the CN. Examples of ServerNameRules entires: • marketing.cisco.com, sales.cisco.com • engineering.cisco.com The wildcard character **"*"** can be used to specify server names with similar characters. For example, ***.cisco.com** matches all the servers in the Cisco.com domain. The wildcard can be placed only at the beginning and the characters that follow the wildcard should be of exact match. More examples with wildcard: • ***.marketing.cisco.com** • ***.com**

Table 9-6 Cisco NAC Agent Verifying Launch Program Executable for Trusted Digital Signature

Registry Key	Default Value (Decimal)	Valid Range	Description/Behavior
SignatureCheck	0	0 or 1	The SignatureCheck setting looks for a digital signature that the Cisco NAC Agent uses to determine whether or not Windows can trust the executable before launching. Starting from Release 4.9(1), non-admin users can set the SignatureCheck parameter to "1" in the Configuration file to check the signature.

For more information, see Configuring a Launch Programs Requirement, page 9-85.

Table 9-7 Additional SWISS Discovery Customization

Parameter	Default Value (Decimal)	Valid Range	Description/Behavior
SwissTimeout	1	> 1	• If this setting is **1**, the Agent performs SWISS discovery as designed and no additional response packet delay timeout value is introduced. • If the setting is an integer **greater than 1**, the Agent waits the additional number of seconds for a SWISS discovery response packet from the Clean Access server before sending another discovery packet to be sure network latency is not delaying the response packet en route.
DisableL3SwissDelay	0	0 or 1	If this setting is 1, the Agent disables its ability to increase the transmission interval for Layer 3 discovery packets. Therefore, the Layer 3 discovery packets repeatedly go out every 5 seconds, just like Layer 2 packets. The default setting for is 0 (enabled). For more information, see the "Layer 3 SWISS Packet Delay to Conserve Bandwidth" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Note SwissTimeout works only for UDP SWISS Timeouts.

Refer to the "Configuring the CAS Managed Network" chapter of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

Table 9-8 HTTP Discovery Customization

Parameter	Default Value (Seconds)	Valid Range	Description/Behavior
HttpDiscoveryTimeout	30	3 and above	The default timeout is 30 seconds. This is the time for which the HTTPS discovery from Agent waits for the response from Clean Access Server. If there is no response for the specified time, then the discovery is timed out. The minimum value that can be set is 3. If the value is set to 1 or 2, the timeout is recognized as 3 seconds. If this value is set to zero (0), then the Windows default timeout settings are used. **Note** In Cisco NAC Appliance 4.9 and later, the HTTPS discovery from Agent checks the network every 30 minutes. In the previous releases, the HTTPS discovery would stop checking after 30 minutes and would resume only when there is a change in the network.
HttpTimeout	120	3 and above	The default timeout is 120 seconds. This is the time for which the HTTP request from Agent waits for the response. If there is no response for the specified time, the request is timed out. The minimum value that can be set is 3. If the value is set to 1 or 2, the timeout is recognized as 3 seconds. If this value is set to zero (0), then the Windows default timeout settings are used. If the value is less than zero (0), the timeout is set to 120 seconds. **Note** HttpTimeout is applied only to posture HTTP communications.

Table 9-9 Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs

Parameter	Default Value (Decimal)	Valid Range	Description/Behavior
RetryDetection	3	0 and above	If ICMP or ARP polling fails, this setting configures the Agent to retry <*x*> times before refreshing the client IP address.
PingArp [1]	0	0-2	• If this value is set to **0**, poll using ICMP. • If this value is set to **1**, poll using ARP. [1] • If this value is set to **2**, poll using ICMP first, then (if ICMP fails) use ARP.

Table 9-9 Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs (continued)

Parameter	Default Value (Decimal)	Valid Range	Description/Behavior
PingMaxTimeout	1	1-10	Poll using ICMP and if no response in <*x*> seconds, then declare ICMP polling failure.
VlanDetectInterval [1]	0 [2], 5 [3]	0, 5-900 [4]	• If this setting is **0**, the Access to Authentication VLAN change feature is disabled. • If this setting is **1-5**, the Agent sends ICMP/ARP queries every 5 seconds. • If this setting is **6-900**, ICMP/ARP every <*x*> seconds.
EnableVlanDetectWithoutUI	0	0,1	This parameter is used to enable the VLAN detect feature when the NAC Agent Tray icon is not running (for example: When the client machine is at the Windows login prompt). This can be used by administrators who have CDL timers setup, to "kick" users out when their machines are powered-on but not logged-in. This would confirm that the machine has a valid IP when the network has changed. • If this value is set to **0**, the VLAN detect feature is disabled. This is the default setting. • If this value is set to **1**, the VLAN detect feature is enabled.

1. VLAN Detect may fail when using ARP as discovery method in situations with high network utilization. Use ICMP as an alternative method.
2. For Windows NAC Agent, the default value is 0. By default, the Access to Authentication VLAN change feature is disabled for Windows.
3. For Mac OS X Agent, the default value is 5. By default, the Access to Authentication VLAN change feature is enabled with “VlanDetectInterval” as 5 seconds for Mac OS X.
4. The maximum range for the Cisco NAC Agent is 900 seconds (15 minutes). The maximum range for the Cisco Clean Access Agent is 60 seconds (1 minute). For more information, refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

Refer to Configure Access to Authentication VLAN Change Detection, page 3-67 for additional details.

Table 9-10 Client-Side MAC Address Management

Parameter	Default Value	Valid Range	Description/Behavior
ExceptionMACList	—	Valid MAC address	If you specify one or more MAC addresses in this setting, the Agent does not advertise those MAC addresses to the CAS during login and authentication to help prevent sending unnecessary MAC addresses over the network. The text string you specify must be a comma-separated list of MAC addresses including colons. For example: `AA:BB:CC:DD:EE:FF,11:22:33:44:55:66`
GeneratedMAC	—	Valid MAC address	This parameter supports Evolution Data Optimized (EVDO) connections on the client machine. If the client machine does not have an active NIC, the Agent creates a "dummy" MAC address for the system.

Table 9-11 Enable or Disable Cisco NAC Agent Accessibility Interaction

Parameter	Default Value (Decimal)	Valid Range	Description/Behavior
AccessibilityMode	0	0 or 1	• If this setting is 1, the Cisco NAC Agent is compatible with the JAWS screen reader. • If this setting is **0**, the Agent does not interact with the JAWS screen reader. **Note** Users may experience a slight impact on performance when this feature is enabled. The Agent still functions normally if this feature is enabled on a client machine that does not have the JAWS screen reader installed.

Refer to *Accessibility Features in Cisco NAC Agent- Keyboard Navigation* for more details.

Table 9-12 Specify Cisco NAC Agent Localization Settings

Parameter	Default Value	Valid Range	Description/Behavior
Locale	OS setting ("**default**")	—	• If this setting is **default**, the Agent uses the Locale settings from the client operating system. • If this setting is either the ID, abbreviated name, or full name of a supported language, the Agent automatically displays the appropriate localized text in Agent dialogs on the client machine.

Table 9-13 Agent Configuration XML File "Locale" Parameter Settings

Language	ID	Abbreviated Name	Full Name
Catalan (Spain)	1027	ca	Catalan
Chinese_simplified	2052	zh-cn	ChineseSimplified
Chinese_traditional	1028	zh-tw	ChineseTraditional
Czech	1029	cs	Czech
Danish	1030	da	Danish
Dutch (Standard)	1043	nl	Dutch
English US	1033	en	English
Finnish	1035	fi	Finnish
French	1036	fr	French
French - Canada	3084	fr-ca	FrenchCanadian
German	1031	de	German
Hungarian	1038	hu	Hungarian
Italian	1040	it	Italian
Japanese	1041	ja	Japanese
Korean (Extended Wansung)	1042	ko	Korean
Norwegian	1044	no	Norwegian
Polish	1045	pl	Polish
Portuguese	2070	pt	Portuguese
Russian	1049	ru	Russian
Serbian (Cyrillic)	3098	src	SerbianCyrillic
Serbian (Latin)	2074	sr	SerbianLatin
Spanish (Traditional)	1034	es	SpanishTraditional
Swedish	1053	sv	Swedish
Turkish	1055	tr	Turkish

Agent Customization File Settings

This section describes how to customize various Cisco NAC Agent features by specifying settings within the Agent customization file (**branding.tar.gz**).

The "**branding.tar.gz**" file usually contains the following files:

- nac_logo.gif
- nac_login.xml
- nacStrings_xx.xml

The following parameters can be customized:

- Logo
- Agent Login Screen
- Predetermined Set of Agent Strings and Fields

Logo

The Cisco logo that appears in all the NAC Agent screens can be replaced with your brand logo. The image should be a .gif file, not exceeding 67 x 40 pixels. The logo image should be named as "nac_logo.gif".

Agent Login Screen

By default, the NAC Agent Login screen appears as shown in Figure 9-8.

Figure 9-8 NAC Agent Login - Default Screen



The elements that appear on the NAC Agent Login screen can be customized by using either one of the following methods:

- Modify the "nac_login.xml" file
- Modify the "nacStrings_xx.xml" file

Note You can replace the default logo by using the "nac_logo.gif" file.

In a system that has NAC Agent installed at the default location, you can find the above files in the following directories:

- The "nac_login.xml" file is available in the "C:\Program Files\Cisco\Cisco NAC Agent\UI\nac_divs\login" directory.

- In the “nacStrings_xx.xml” file, the “xx” indicates the locale. You can find a complete list of the files in the “C:\Program Files\Cisco\Cisco NAC Agent\UI\cues_utility” directory.

Note The files are available in the directories mentioned above when the Agent is installed at the default location. If the Agent is installed at a different location, then the files would be available at “<Agent Installed path>\Cisco\Cisco NAC Agent\UI\nac_divs\login” and “<Agent Installed path>\Cisco\Cisco NAC Agent\cues_utility”.

Tip Cisco recommends to make changes in the “nacStrings_xx.xml” file.

The following example shows a part of contents of the “nac_login.xml” file. The customized text is shown in boldface.

```
<tr class="nacLoginMiddleSectionContainerInput">
   <td colspan="2">
      <fieldset width="100%" id="nacLoginCustomAlert"
                style="display:block" class="nacLoginAlertBox">
          <table width="100%">
             <tr>
                <td id="nacLoginCustomAlert.img" valign="top" width="32px">
                  <img src="./cues_icons/Status_warning_icon.png" align="absmiddle"
onload="cuesFixPNG(null,this)"></img>
                </td>
                <td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
                  <cues:localize key="login.customalert"/>
                </td>
              </tr>
          </table>
       </fieldset>
    </td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
    <td>
       <cues:localize key="cd.nbsp"/>
    </td>
    <td class="cuesLoginField" >
      <nobr>
      <input type="checkbox" alt="" title="" name="rememberme"
             id="rememberme" checked="true" />
            <cues:localize key="login.remember_me"/>
      </nobr>
    </td>
</tr>
```

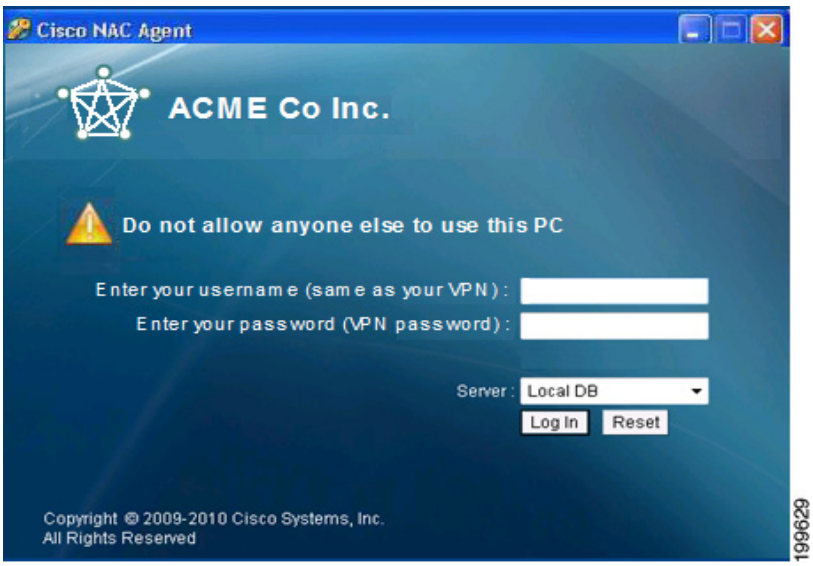
The following example shows a part of contents of “nacStrings_xx.xml” file. The customized text is shown in boldface.

```
<cueslookup:name key="login.productname"> ACME Co Inc. </cueslookup:name>
<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.username"> Enter your username (same as your VPN)
</cueslookup:name>
<cueslookup:name key="login.password">Enter your password (VPN password)</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Do not allow anyone else to use this
PC</cueslookup:name>
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
```

```
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
```

The above file has been modified to customize the login screen as shown in Figure 9-9.

Figure 9-9 Cisco NAC Agent Login—Customized Screen



Notice that the “Remember Me” checkbox has been removed. In addition, you can find more text for the “Username” and “Password” fields.

Note Though there is no limit for the number of characters used for the customized text, it is recommended to restrict them so that they are not occupying too much of space in the Login screen.

Predetermined Set of Agent Strings and Fields

Modify the “nacStrings_xx.xml” file to replace the Device Posture Status (DPS) details. The following is a part of the “nacStrings_xx.xml” file with DPS values.

Example nacStrings_xx.xml File:

```
<cueslookup:name key="dp.status.fullNetAccess">Full Network Access</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">Your device conforms with all the
security policies for this protected network</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">Refreshing IP address. Please
Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">Refreshing IP address
succeeded.</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">Connecting to protected
Network. Please Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">Guest Network Access</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">Network Access Denied</cueslookup:name>
```

```
<cueslookup:name key="dp.status.noNetAccess.verbose">There is at least one mandatory
requirement failing. You are required to update your system before you can access the
network.</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">Network Usage Terms and
Conditions are rejected. You will not be allowed to access the network.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">Restricted Network Access
granted.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">You have been granted
restricted network access because your device did not conform with all the security
policies for this protected network and you have opted to defer updating your system. It
is recommended that you update your system at your earliest convenience.</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">Temporary Network
Access</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">Please be patient
while your system is checked against the network security policy.</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">There is at least one
mandatory requirement failing. You are required to update your system otherwise your
network access will be restricted.</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">Only optional requirements
are failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">Temporary Access to the network
has expired.</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose"> </cueslookup:name>
```

Note The strings need to be replaced in every locale for which the customization is required. If customization is required for more than one locales, then the modification has to be done in more than one **nacStrings_xx.xml** file.

After modifying the required files, tar all the files and save the tarred file as "**branding.tar.gz**". The following is an example of the tar command:

```
tar cvzf branding.tar.gz nac_login.xml nac_logo.gif nacStrings_en.xml
```

Upload the tar file to the client system using the **Agent Installation** option in the CAM. See Installation Page, page 9-20 for more details.

If you are using Altiris/SMS, you can distribute the customization files along with the MSI package. Refer to Cisco NAC Agent MSI Installer, page 9-37 for more information.

When using the MSI package, distribute the individual customization files (nac_login.xml, nac_logo.gif, and nacStrings_en.xml) and not the "branding.tar.gz" file.

Cisco NAC Agent MSI Installer

Cisco NAC Appliance provides an MSI (Microsoft Installer format) installer for the Cisco NAC Agent (called **nacagentsetup-win.msi**) on Windows client machines. There is also a .zip version of the same installer package that uses up less local memory on file transfer. You can download the MSI and/or .zip package from the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. Once you have obtained the Cisco NAC Agent MSI or .zip package, you can place the MSI installer in

a directory on the client machine along with an Agent configuration XML file (**NACAgentCFG.xml**) containing the appropriate Discovery Host address telling the client machine where to look for the Cisco NAC Appliance network.

Step 1 Download the **nacagentsetup-win.msi** or **nacagentsetup-win.zip** installer file from the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml.

Step 2 Place the **nacagentsetup-win.msi** file in a specific directory on the client machine (for example, C:\temp\nacagentsetup-win.msi):

- If you are copying the MSI installer directly over to the client, place the **nacagentsetup-win.msi** file into a directory on the client machine from which you plan to install the Cisco NAC Agent.
- If you are using the **nacagentsetup-win.zip** installer, extract the contents of the .zip file into the directory on the client machine from which you plan to install the Cisco NAC Agent

Step 3 Place an Agent configuration XML file specifying the appropriate Discovery Host address in the same directory as the Cisco NAC Agent MSI package. For information on the Agent configuration XML file and its parameters and syntax, see Cisco NAC Agent XML Configuration File Settings, page 9-23.

As long as the Agent configuration XML file exists in the same directory as the MSI installer package, the installation process automatically places the Agent configuration XML file in the appropriate Cisco NAC Agent application directory so the Agent can point to the correct network location when it is first launched.

Note The Discovery Host field can be made editable or not by changing the DiscoveryHostEditable parameter in the Agent configuration XML file. See Cisco NAC Agent XML Configuration File Settings, page 9-23 for more details.

Step 4 Open a Command prompt on the client machine and enter the following to execute the installation:

```
msiexec.exe /i NACAgentSetup-win.msi /qn /l*v c:\temp\agent-install.log
```

Note The `/qn` qualifier installs the Cisco NAC Agent completely silently. The `/l*v` logs the installation session in verbose mode.

The Cisco NAC Agent is installed on the client machine and automatically launches in the background using the Discovery Host supplied in the Agent configuration XML file to contact the Cisco NAC Appliance network.

If you are using Altiris/SMS to distribute the MSI installer, perform the following to enforce Agent Customization.

- Place the Agent customization files in a sub-directory named "brand" in the directory “%TEMP%/CCAA”.
- When the NAC Agent is installed in the client, the customization is applied to the Agent.
- To remove the customization, send a plain MSI without the customization files.

To know more about the Agent customization files, see Agent Customization File Settings, page 9-33.

Configuring Agent-Based Posture Assessment

This section describes how to configure requirements on the CAM so that the Agent can perform posture assessment and remediation on client machines.

- Overview, page 9-1
- Configuring AV/AS Definition Update Requirements, page 9-41
- Configuring a Windows Server Update Services Requirement, page 9-57
- Configuring a Windows Update Requirement, page 9-64
- Configuring Custom Checks, Rules, and Requirements, page 9-70
- Configuring a Launch Programs Requirement, page 9-85
- Map Requirements to Rules, page 9-90
- Apply Requirements to User Roles, page 9-92
- Configuring Auto Remediation for Requirements, page 9-98

Overview

To work with a Windows 8.1 client, you need to download and apply a patch. Refer to *Release Notes for Cisco NAC Appliance, Version 4.9(4)* for more information.

Requirements

To perform posture assessment for client machines running the Cisco NAC Agent or Cisco NAC Web Agent, you need to configure and implement requirements based on the type of client validation you want to perform for the client operating system. Requirements are used to implement business-level decisions about what users must (or must not) have running on their systems to be able to access the network. The requirement mechanism maps one or more rules that you want clients in a user role to meet to the action you want those users to take if the client fails the rules. When you create a new requirement, you choose from one of several different requirement types (e.g. AV Definition Update) to configure options, buttons, and remediation instructions the Agent dialogs present to the user when the client fails the requirement. For detailed instructions on creating the different requirement types, see:

- Configuring AV/AS Definition Update Requirements, page 9-41
- Configuring a Windows Server Update Services Requirement, page 9-57
- Configuring a Windows Update Requirement, page 9-64
- Configuring Custom Checks, Rules, and Requirements, page 9-70
- Configuring a Launch Programs Requirement, page 9-85



Note Most requirement remediation actions (like Windows Updates and AV/AS support updates) require the user to have administrator privileges on the client machine. Therefore, Cisco recommends you ensure that users of client machines undergoing posture assessment and remediation have administrator-level privileges.

Rules

In all but one case—the Windows Server Update Service (WSUS) "Severity" option requirement type—you *must* map rules to requirements to ensure client machines meet security standards. A rule is the unit the Agent uses to validate client machines and assess whether or not a requirement has been met. Rules can be:

- Preconfigured AV/AS rules, which you associate to AV/AS requirements. These require no additional checks to validate client machines.
- Preconfigured Cisco Rules ("pr_rule") that feature one or more preset checks. For example, Windows hotfix-related "pr_" rules that only address "Critical" updates. You can map pr_rules as the validation criteria for several different requirement types. Refer to Cisco Pre-Configured Rules ("pr_"), page 9-71 for further details on Cisco Rules.
- A custom rule made up of one or more preconfigured or custom checks. A custom rule is one you create yourself by configuring a rule expression based on checks.

For details on mapping requirements to rules, see Map Requirements to Rules, page 9-90.

Checks

Checks are the building blocks for rules, but in most cases you will not need to configure them. A check is a single registry, file, service, or application check for a selected operating system, and is used to create a custom rule. A check can be a Cisco pre-configured check (pc_ check) or a custom check you create yourself. When you map rules to requirements, make sure the appropriate checks (pc_ checks or custom checks) are in place to accurately validate client machines.



Note Preconfigured ("pr_") rules are already associated with one or more checks that validate client machine security standards. You only need to create custom rules or checks if the preconfigured rules or checks do not meet your needs. See Configuring Custom Checks, Rules, and Requirements, page 9-70 for more information.

Role Mapping

Once you have mapped a requirement to one or more rules, the final step is to associate the requirement to a normal login user role. Users who attempt to authenticate into the normal user role are put into the Temporary role until they pass requirements associated with the normal login role:

- If they successfully meet the requirements, the users are allowed on the network in the normal login role.
- If they fail to meet the requirements, users stay in the Temporary role for the session timeout until they take the steps described in the Agent dialogs and successfully meet the requirements.

For details on mapping requirements to roles, see Apply Requirements to User Roles, page 9-92.

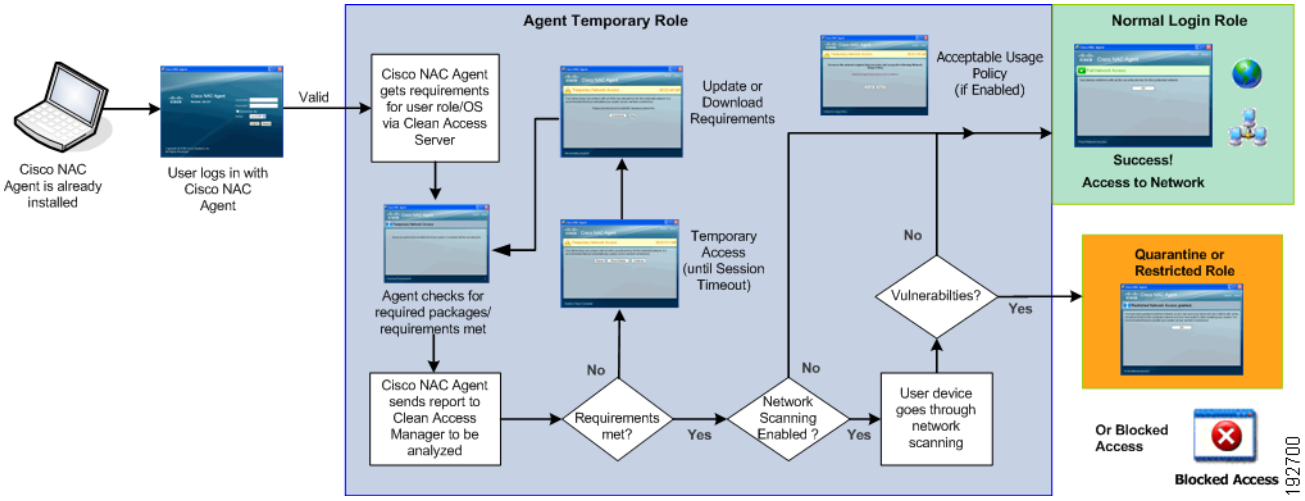


Note To map a requirement to a normal login user role, the role must already be created as described in Create User Roles, page 6-2.

Agent Posture Assessment Process

Figure 9-10 details the Cisco NAC Appliance client posture assessment process (with or without network scanning) when a user authenticates via the Agent.

Figure 9-10 Agent Posture Assessment



The following user roles are used for Cisco NAC Appliance and must be configured with traffic policies and session timeout:

- **Unauthenticated Role**—Default system role for unauthenticated users (Agent or web login) behind a Clean Access Server. Web login users are in the unauthenticated role while network scanning is performed.
- **Agent Temporary Role**—Agent users are in the Temporary role while Agent requirements are checked on their systems.
- **Quarantine Role**—Both web login and Agent users are put in the Quarantine role when network scanning determines that the client machine has vulnerabilities.

If a user meets Agent requirements and/or has no network scanning vulnerabilities, the user is allowed access to the network in the normal login user role or "restricted access" role. See Client Posture Assessment Roles, page 6-5 for additional details.

During user login/remediation, the Agent dialogs present different buttons that users can click depending on the type of Agent installed and the requirement(s) assigned to validate the client machine. For specific information on Agent dialogs and behavior, see Chapter 10, "Cisco NAC Appliance Agents."

Configuring AV/AS Definition Update Requirements

The **AV Definition Update** and **AS Definition Update** requirement type can be used to report on and update the definition files on a client for supported antivirus or antispyware products. If the client fails to meet the AV/AS requirement, the Agent communicates directly with the installed antivirus or antispyware software on the client and automatically updates the definition files when the user clicks the **Update/Remediate** button on the Agent dialog.

Note The Cisco NAC Web Agent only supports **Go To Link** manual remediation and **File Distribution** functionality. Cisco NAC Web Agent does not support **Update** or **Launch** remediation actions, nor does it perform Auto Remediation.

AV Rules incorporate extensive logic for antivirus vendors and are associated with AV Definition Update requirements. AS Rules incorporate logic for most antispyware vendors and are associated with AS Definition Update requirements. For AV or AS Definition Update requirements, there is no need to configure checks. You associate:

- AV Definition Update requirement with AV Rule(s) and user roles and operating systems
- AS Definition Update requirement with AS Rule(s) and user roles and operating systems

and configure the Agent dialog instructions you want the user to see if the AV or AS requirement fails.

Note Where possible, Cisco recommends using AV Rules mapped to AV Definition Update Requirements to check antivirus software on clients. In the case of a non-supported AV product, or if an AV product/version is not available through AV Rules, administrators always have the option of using Cisco provided pc_ checks and pr_rules for the AntiVirus vendor or of creating their own custom checks, rules, and requirements through **Device Management > Clean Access > Clean Access Agent** (use New Check, New Rule, and New File/Link/Local Check Requirement), as described in Configuring Custom Checks, Rules, and Requirements, page 9-70.

Cisco NAC Appliance works in tandem with the installation schemes and mechanisms provided by supported Antivirus vendors. In the case of unforeseen changes to underlying mechanisms for AV products by AV vendors, the Clean Access team updates the Supported AV/AS Product List and/or Agent in the timeliest manner possible in order to support the new AV product changes. In the meantime, administrators can always use the “custom” rule workaround for the AV product (such as pc_checks/pr_rules) and configure the requirement for “Any selected rule succeeds.”

Figure 9-11 and Figure 9-12 show Agent dialogs that appear when a client fails to meet an AV Definition Update requirement.

Figure 9-11 Required AV Definition Update (Cisco NAC Agent)

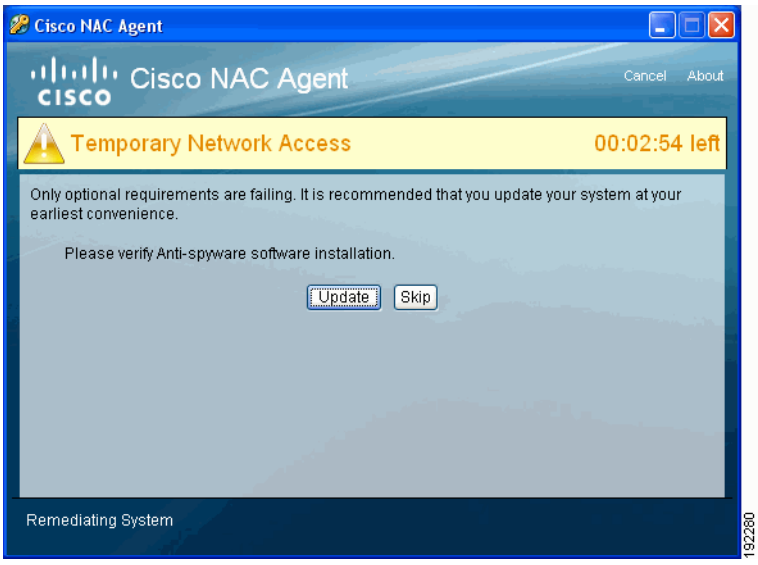
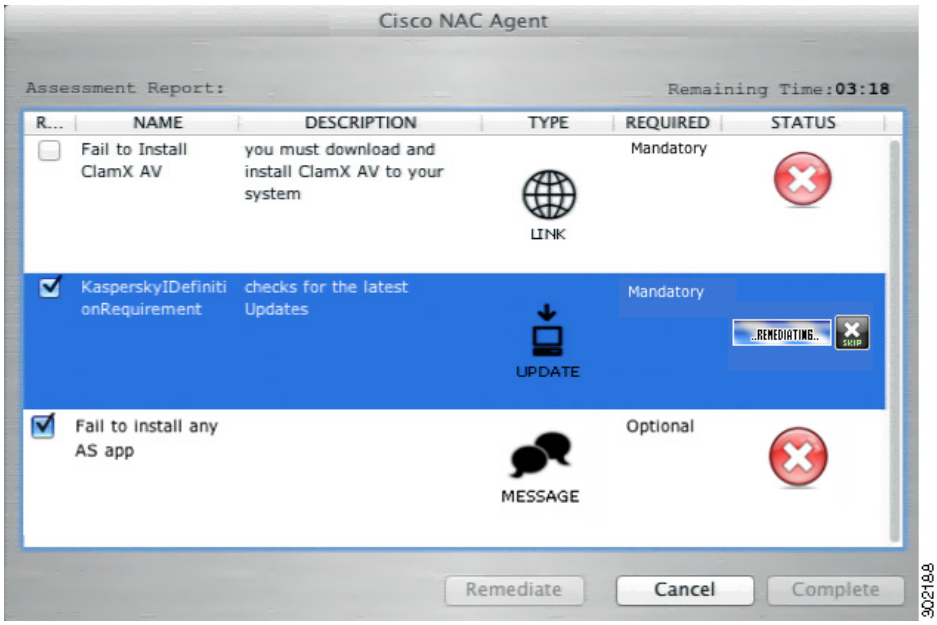


Figure 9-12 Required AV Definition Update (Mac OS X Agent)



AV Rules and AS Rules

Antivirus rules (AV Rule) and anti-spyware rules (AS Rule) are preconfigured rule types that are mapped to the matrix of vendors and products sourced in the Supported AV/AS Product List. There is no need to configure checks with this type of rule.

There are two basic types of AV Rules:

- **Installation AV Rules** check whether the selected antivirus software is installed for the client operating systems.
- **Virus Definition AV Rules** check whether the virus definition files are up-to-date on the client. Virus Definition AV Rules can be mapped into AV Definition Update requirements so that a user that fails the requirement can automatically execute the update by clicking the **Update** button in the Agent and the system reporting function can alert Cisco NAC Web Agent users of the requirement.

There are two basic types of AS Rules:

- **Installation AS Rules** check whether the selected anti-spyware software is installed for the client OS.
- **Spyware Definition AS Rules** check whether the spyware definition files are up-to-date on the client. Spyware Definition AS Rules can be mapped into AS Definition Update requirements so that a user that fails the requirement can automatically execute the update by clicking the **Update** button in the Agent and the system reporting function can alert Cisco NAC Web Agent users of the requirement.

Note In some cases, the specific AV/AS vendor software requires the user to have administrator privileges on the client machine to enable updates.

- **AV Rules** are typically associated with **AV Definition Update** requirements, and **AS Rules** are typically associated with **AS Definition Update** requirements.

The steps to create AV Definition Update Requirements are as follows:

Step 1 Verify AV/AS Support Info, page 9-44

Step 2 Create an AV Rule, page 9-47

Step 3 Create an AV Definition Update Requirement, page 9-50

Step 4 Map Requirements to Rules, page 9-90

Step 5 Apply Requirements to User Roles, page 9-92

Step 6 Validate Requirements, page 9-93

The steps to create AS Definition Update Requirements are as follows:

Step 1 Verify AV/AS Support Info, page 9-44

Step 2 Create an AS Rule, page 9-53

Step 3 Create an AS Definition Update Requirement, page 9-55

Step 4 Map Requirements to Rules, page 9-90

Step 5 Apply Requirements to User Roles, page 9-92

Step 6 Validate Requirements, page 9-93

Note In some cases it may be advantageous to configure AV or AS rules/requirements in different ways. For example:

- Not all product versions of a particular vendor may support the Agent launching the automatic update of the product. In this case, you can provide instructions (via the Description field of the AV or AS Definition Update requirement) to have users update their AV or AS definition files from the interface of their installed AV or AS product.
- You can associate the AV or AS rules with a different requirement type, such as Link Distribution or Local Check, to change the Agent buttons and user action required from "Update" to "Go to Link", or to disable the action button and provide instructions only. This allows you flexibility in configuring the actions you want your users to take.
- You can also configure different Enforce Types. You can generate reports for clients and optionally provide users extra time to meet a requirement without blocking them from the network. See Configuring an Optional/Audit Requirement, page 9-94 for details.

Verify AV/AS Support Info

Cisco NAC Appliance allows multiple versions of the Agent to be used on the network. New updates to the Agent will add support for the latest antivirus or antispyware products as they are released. The system picks the best method (either Def Date or Def Version) to execute AV/AS definition checks based on the AV/AS products available and the version of the Agent. The **AV/AS Support Info** page provides details on Agent compatibility with the latest Supported AV/AS Product List downloaded to the CAM. This page lists the latest version and date of definition files for each AV and AS product as well the

baseline version of the Agent needed for product support. You can compare the client's AV or AS information against the **AV/AS Support Info** page to verify if a client's definition file is the latest. If running multiple versions of the Agent on your network, this page can help troubleshoot which version must be run to support a particular product.

Use the following steps to view Agent support details.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.

Step 2 Choose either **Antivirus** (Figure 9-13 and Figure 9-14) or **Anti-Spyware** (Figure 9-15 and Figure 9-16) from the Category dropdown.

Figure 9-13 AV/AS Support Info — Windows AV Vendor Example

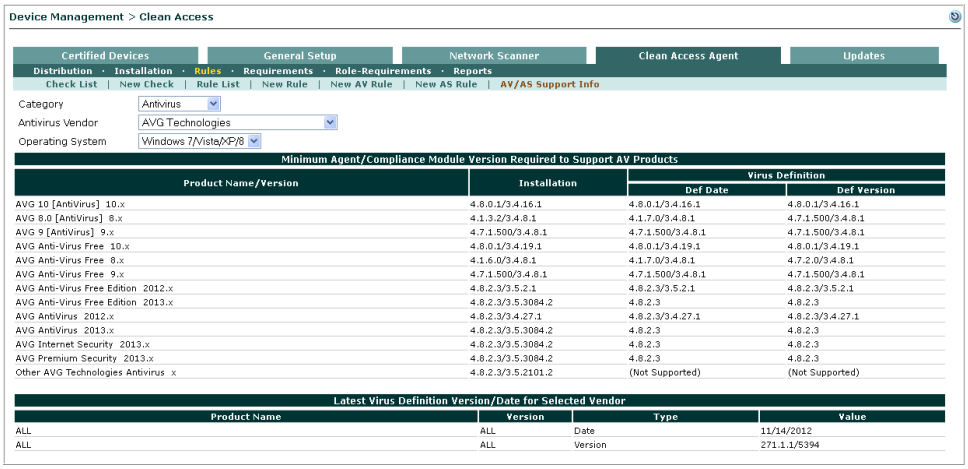

Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Distribution · Installation · Rules · Requirements · Role-Requirements · Reports
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Category
Antivirus
Antivirus Vendor
AVG Technologies
Operating System
Windows 7/Vista/XP/8
Minimum Agent/Compliance Module Version Required to Support AV Products
Product Name/Version
Installation
Virus Definition
Def Date
Def Version
AVG 10 [AntiVirus] 10.x 4.8.0.1/3.4.16.1 4.8.0.1/3.4.16.1 4.8.0.1/3.4.16.1
AVG 8.0 [AntiVirus] 8.x 4.1.3.2/3.4.8.1 4.1.7.0/3.4.8.1 4.7.1.500/3.4.8.1
AVG 9 [AntiVirus] 9.x 4.7.1.500/3.4.8.1 4.7.1.500/3.4.8.1 4.7.1.500/3.4.8.1
AVG Anti-Virus Free 10.x 4.8.0.1/3.4.19.1 4.8.0.1/3.4.19.1 4.8.0.1/3.4.19.1
AVG Anti-Virus Free 8.x 4.1.6.0/3.4.8.1 4.1.7.0/3.4.8.1 4.7.2.0/3.4.8.1
AVG Anti-Virus Free 9.x 4.7.1.500/3.4.8.1 4.7.1.500/3.4.8.1 4.7.1.500/3.4.8.1
AVG Anti-Virus Free Edition 2012.x 4.8.2.3/3.5.2.1 4.8.2.3/3.5.2.1 4.8.2.3/3.5.2.1
AVG Anti-Virus Free Edition 2013.x 4.8.2.3/3.5.3084.2 4.8.2.3 4.8.2.3
AVG AntiVirus 2012.x 4.8.2.3/3.4.27.1 4.8.2.3/3.4.27.1 4.8.2.3/3.4.27.1
AVG AntiVirus 2013.x 4.8.2.3/3.5.3084.2 4.8.2.3 4.8.2.3
AVG Internet Security 2013.x 4.8.2.3/3.5.3084.2 4.8.2.3 4.8.2.3
AVG Premium Security 2013.x 4.8.2.3/3.5.3084.2 4.8.2.3 4.8.2.3
Other AVG Technologies Antivirus x 4.8.2.3/3.5.2101.2 (Not Supported) (Not Supported)
Latest Virus Definition Version/Date for Selected Vendor
Product Name
Version
Type
Value
ALL ALL Date 11/14/2012
ALL ALL Version 271.1.1/5394
303214

Figure 9-14 AV/AS Support Info — Mac OS X AV Vendor Example

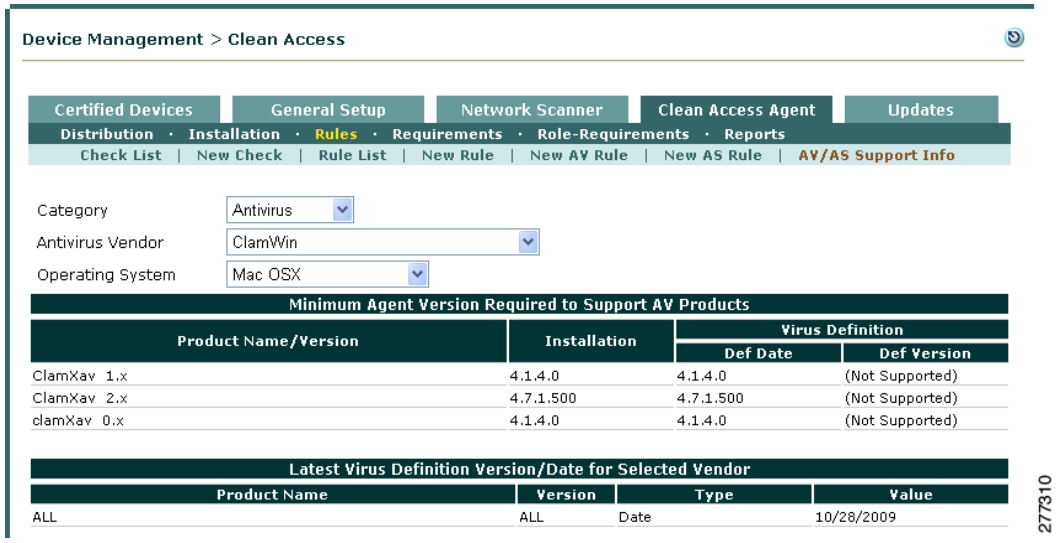


Figure 9-15 AV/AS Support Info — Windows AS Vendor Example

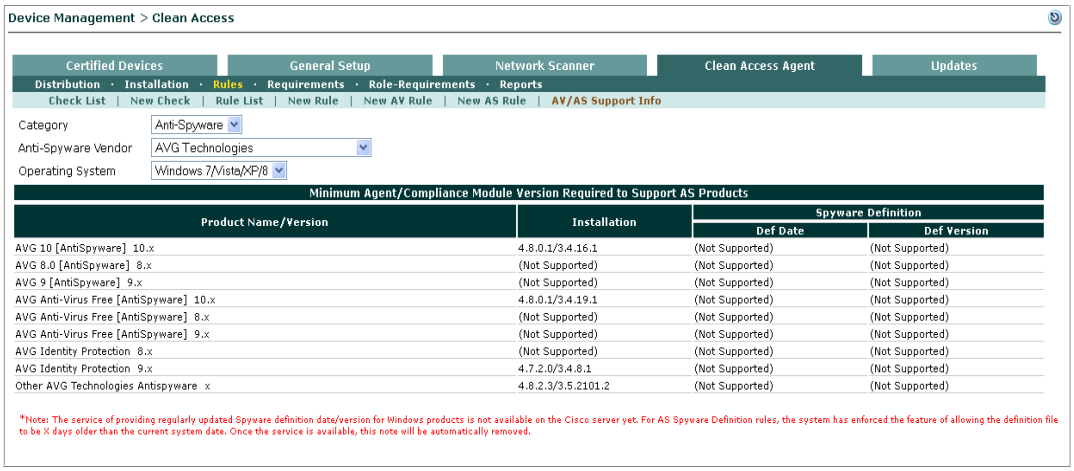
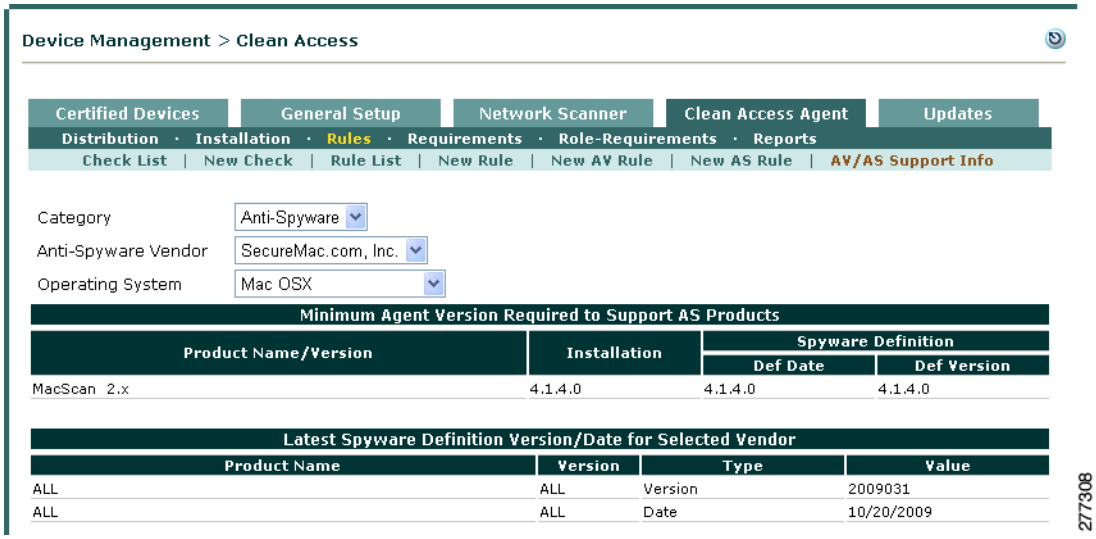

Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Distribution · Installation · Rules · Requirements · Role-Requirements · Reports
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Category
Anti-Spyware
Anti-Spyware Vendor
AVG Technologies
Operating System
Windows 7/Vista/XP/8
Minimum Agent/Compliance Module Version Required to Support AS Products
Product Name/Version
Installation
Spyware Definition
Def Date
Def Version
AVG 10 [AntiSpyware] 10.x
4.8.0.1/3.4.16.1
(Not Supported)
AVG 8.0 [AntiSpyware] 8.x
AVG 9 [AntiSpyware] 9.x
AVG Anti-Virus Free [AntiSpyware] 10.x
4.8.0.1/3.4.19.1
AVG Anti-Virus Free [AntiSpyware] 8.x
AVG Anti-Virus Free [AntiSpyware] 9.x
AVG Identity Protection 8.x
AVG Identity Protection 9.x
4.7.2.0/3.4.8.1
Other AVG Technologies Antispyware x
4.8.2.3/3.5.2101.2
*Note: The service of providing regularly updated Spyware definition date/version for Windows products is not available on the Cisco server yet. For AS Spyware Definition rules, the system has enforced the feature of allowing the definition file to be X days older than the current system date. Once the service is available, this note will be automatically removed.
303213

Figure 9-16 AV/AS Support Info — Mac OS X AS Vendor Example



Step 3 Choose a corresponding vendor (**Antivirus Vendor** or **Anti-Spyware Vendor)** from the dropdown menu.

Note Regular updates for Anti-Spyware definition date/version will be made available via Cisco Updates. Until update service is available, the system enforces definition files to be *x* days older than the current system date for AS Spyware Definition rules (under **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**).

Step 4 Choose one of the following operating systems from the **Operating System** dropdown menu to view the support information for those client systems:

- **Windows 8.1/8/7/Vista/XP**
- **Mac OSX**

Check the **Minimum Agent Version Required to Support AV/AS Products** table for product details.

Your selection populates the following tables:

- **Minimum Agent Version Required to Support AV/AS Products**: shows the minimum Agent version required to support each AV/AS product. For example:
  - A 4.1.3.0 or later Windows Agent can log into a role that requires Aluria Security Center AntiVirus 1.x, but for any earlier Agent version, this check will fail.
  - A 4.6.0.3 Mac OS X Agent can log into clamXav: 0.x and ClamXav: 1.x.

  Note that if a version of the Agent supports both Def Date and Def Version checks, the Def Version check will be used.
- **Latest Virus/Spyware Definition Version/Date for Selected Vendor**: displays the latest version and date information for the AV/AS product. The AV software for an up-to-date client should display the same values.

Note The Agent sends its version information to the CAM, and the CAM always attempts to first use the virus definition version for AV checks. If the version is not available, the CAM uses the virus definition date instead.

Tip You can also view the latest def file version when selecting an AV vendor from the **New AV Rule** form.

Create an AV Rule

Note Your CAM/CAS must be running Cisco NAC Appliance release 4.5 or later and have the latest Cisco AV/AS support updates in order to perform client remediation using version 4.5.0.0+ of the Mac OS X Agent.

Use the following steps to configure an AV rule.

Step 1 Make sure you have the latest version of the Supported AV/AS Product List, as described in Retrieving Cisco NAC Appliance Updates, page 9-12.

Step 2 Go to **Device Management > Clean Access > Clean Access Agent > Rules > New AV Rule**.

Figure 9-17 New AV Rule—Windows

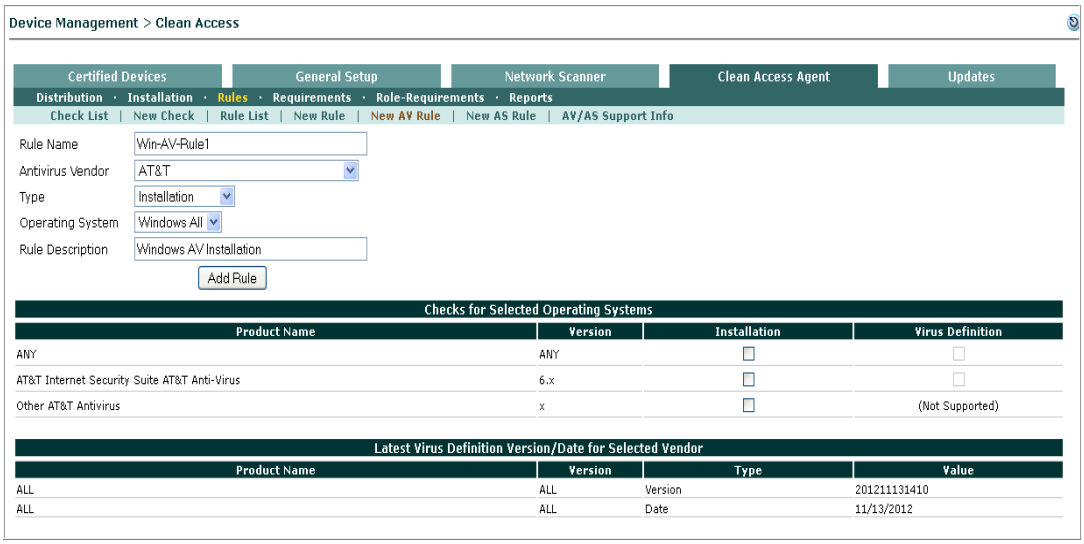
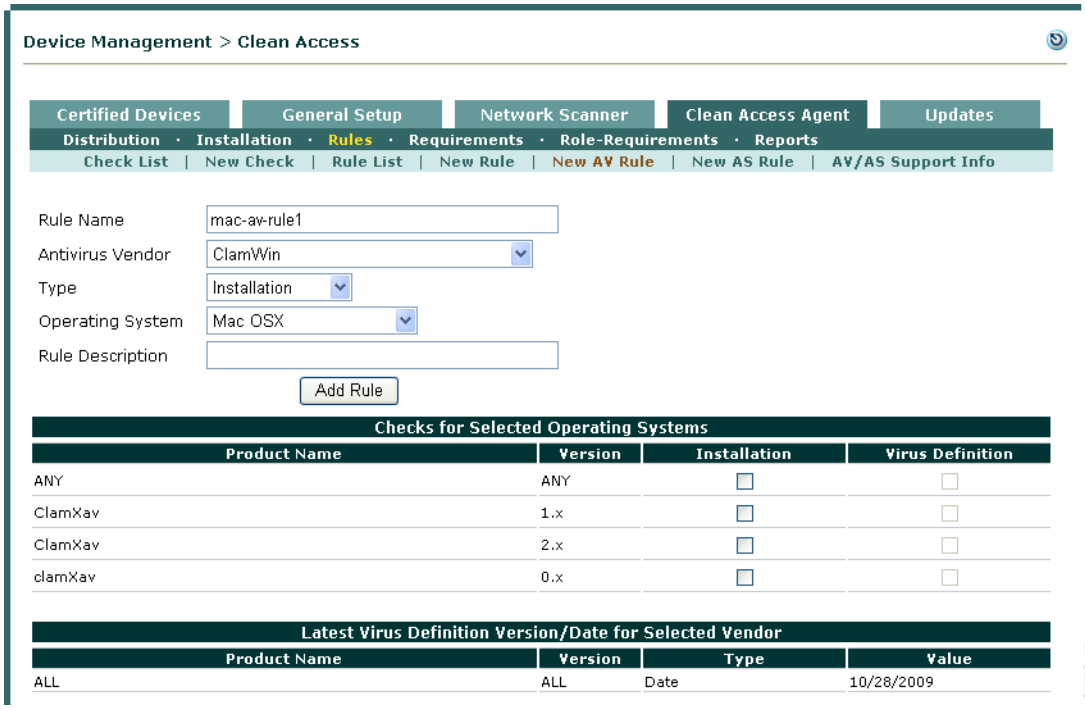


Figure 9-18 New AV Rule—Mac OS X



Step 3 Type a **Rule Name**. You can use digits and underscores, but no spaces in the name.

Step 4 Choose a specific **Antivirus Vendor**, or choose **ANY** vendor, from the dropdown menu. Along with the **Operating System** chosen, this populates the **Checks for Selected Operating Systems** table at the bottom of the page for the **ANY** vendor option or with the supported products and product versions for the specified vendor.

Note Cisco recommends specifying vendor names when appropriate because choosing the **ANY** option can affect the Agent's performance (the process takes longer) on the client machine.

Step 5 From the **Type** dropdown menu, choose either **Installation** or **Virus Definition**. This enables the checkboxes for the corresponding Installation or Virus Definition column in the table below.

Step 6 Choose an **Operating System** from the dropdown menu. This populates the product versions supported for this client OS in the table below:

- **Windows 8.1/8/7/Vista/XP**
- **Mac OSX**

Step 7 Type an optional **Rule Description**.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

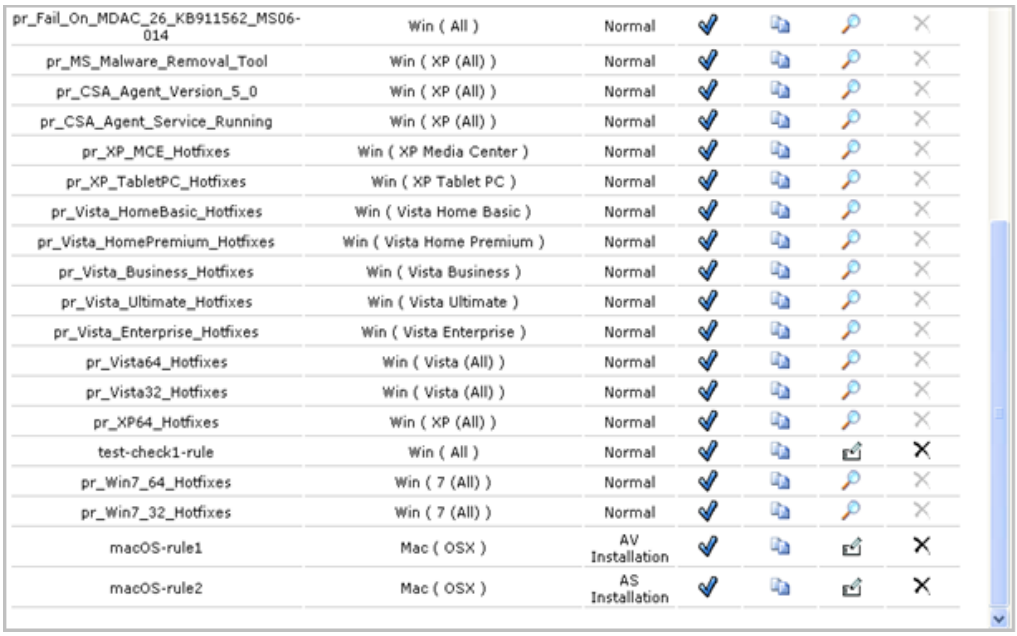
Step 8 In the **Checks for Selected Operating Systems** table, choose the product versions you want to check for on the client by clicking the checkbox(es) in the corresponding **Installation** or **Virus Definition** column:

- **ANY** means you want to check for any product and any version from this AV vendor.
- **Installation** checks whether the product is installed.
- **Virus Definition** checks whether the virus definition files are up to date on the client for the specified product.

Note In a definition rule, the Agent first confirms whether or not the product is installed, then checks whether or not the definition file is up-to-date.

Step 9 Click **Add Rule**. The new AV rule will be added at the bottom of the **Rule List** with the name you provided.

Figure 9-19 New AV Rules Appear at the Bottom of the Rule List—Mac OS X Example


pr_Fail_On_MDAC_26_KB911562_MS06-014 Win (All) Normal
pr_MS_Malware_Removal_Tool Win (XP (All)) Normal
pr_CSA_Agent_Version_5_0 Win (XP (All)) Normal
pr_CSA_Agent_Service_Running Win (XP (All)) Normal
pr_XP_MCE_Hotfixes Win (XP Media Center) Normal
pr_XP_TabletPC_Hotfixes Win (XP Tablet PC) Normal
pr_Vista_HomeBasic_Hotfixes Win (Vista Home Basic) Normal
pr_Vista_HomePremium_Hotfixes Win (Vista Home Premium) Normal
pr_Vista_Business_Hotfixes Win (Vista Business) Normal
pr_Vista_Ultimate_Hotfixes Win (Vista Ultimate) Normal
pr_Vista_Enterprise_Hotfixes Win (Vista Enterprise) Normal
pr_Vista64_Hotfixes Win (Vista (All)) Normal
pr_Vista32_Hotfixes Win (Vista (All)) Normal
pr_XP64_Hotfixes Win (XP (All)) Normal
test-check1-rule Win (All) Normal
pr_Win7_64_Hotfixes Win (7 (All)) Normal
pr_Win7_32_Hotfixes Win (7 (All)) Normal
macOS-rule1 Mac (OSX) AV Installation
macOS-rule2 Mac (OSX) AS Installation
236835

Note When configuring AV Rules, the “ANY” Antivirus vendor option and the vendor-specific “ANY Product/ANY Version” option work differently:

- For ANY vendor, the Agent needs to query the server to verify whether the installed products are from a supported vendor. Because the Agent only queries once at the beginning of each login session, the user must click **Cancel** or restart the Agent to repeat the login process in order to refresh the server's response.
- For “ANY Product/ANY Version” for a specific vendor, the Agent only needs to match the required vendor against what is installed on the client machine. No query is needed.

Create an AV Definition Update Requirement

The following steps show how to create a new AV Definition Update requirement to check the client system for the specified AV product(s) and version(s) using an associated AV Rule. If the client’s AV definition files are not up-to-date, the user can simply click the **Update/Remediate** button on the Agent, and the Agent causes the resident AV software launch its own update mechanism. Note that the actual mechanism differs for different AV products (e.g. live update vs.command line parameter).

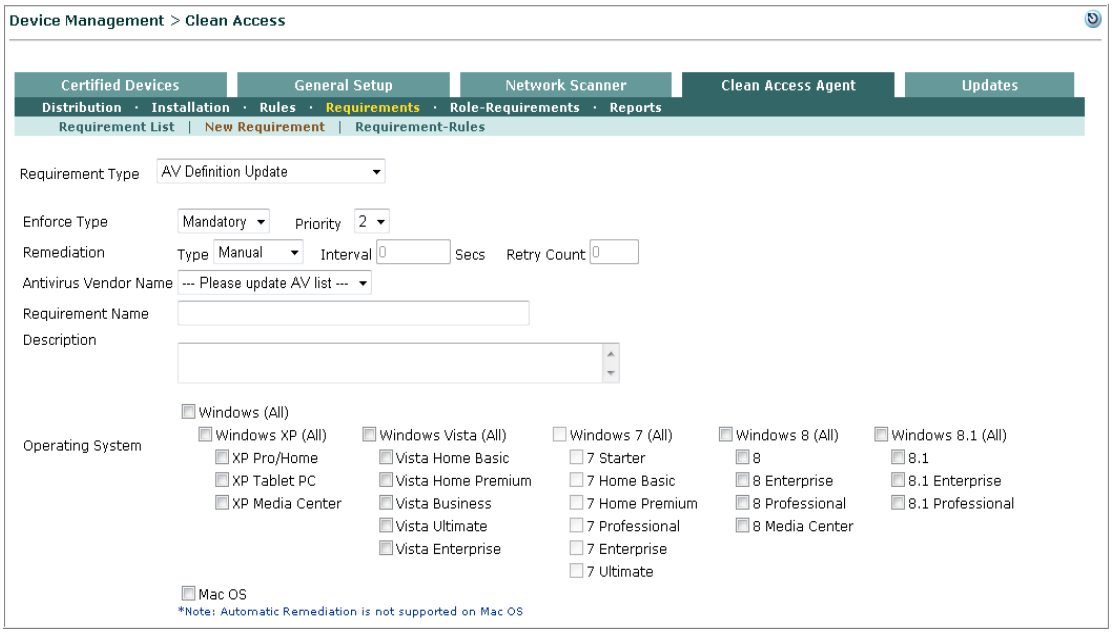
Note The Cisco NAC Web Agent only supports **Go To Link** manual remediation and **File Distribution** functionality. Cisco NAC Web Agent does not support **Update** or **Launch** remediation actions, nor does it perform Auto Remediation.

Note Mac OS X users can only resolve ClamWin AV Definition Update requirements by navigating to the ClamXAV download site at http://www.clamav.net. Cisco recommends using the pre-defined host policy list for the Unauthenticated Role on the CAM (**User Management > User Roles > Traffic Control > Host**).

Use the following steps to create an AV Definition Update requirement.

Step 1 In the **Clean Access Agent** tab, click the **Requirements** submenu link and then **New Requirement**.

Figure 9-20 New Requirement



Step 2 For **Requirement Type** choose **AV Definition Update**.

Step 3 Choose an **Enforce Type** from the dropdown menu:

- **Mandatory**—Enforce requirement.The user is informed of this requirement and cannot proceed or have network access unless the client system meets it.
- **Optional**— Do not enforce requirement. The user is informed of the requirement but can bypass it if desired (by clicking **Next/Skip** in the Agent dialog). The client system does not have to meet the requirement for the user to proceed or have network access.
- **Audit**—Silently audit. The client system is checked "silently" for the requirement without notifying the user and a report is automatically generated and sent back to the CAS. (Audit requirements do not appear in the user's Mac OS X Assessment Report window.) The report results (pass or fail) do not affect user network access.

  Refer to Configuring an Optional/Audit Requirement, page 9-94 for details.

Step 4 Choose the **Priority** of execution for this requirement on the client. A high priority (e.g. 1) means this requirement is checked on the system ahead of all other requirements (and appears in the Agent dialogs in that order). Note that if a Mandatory requirement fails, the Agent does not continue past that point until that requirement succeeds.

Note The Mac OS X Agent does not support automatic remediation. Therefore, the Remediation functions that appear on the New Requirement configuration page (Remediation **Type**, **Interval**, and **Retry Count**) do not serve any purpose when creating requirement types for Macintosh client remediation.

Step 5 If you want to enable and configure Auto Remediation for the Agent:

a. Choose the **Remediation Type [Manual | Automatic]** from the dropdown menu. Choosing **Manual** preserves previous Agent behavior. The user has to click through each of the requirements using the **Next/Skip** button in the Agent. Choosing **Automatic** sets the Agent to perform Auto Remediation, where the Agent automatically performs updates or launches required programs on the client after the user logs in.

b. If you configure the requirement to use automatic remediation, specify the **Interval** in seconds (the default interval is 0). Depending on the requirement type, this interval either sets the delay before the Agent re-attempts remediation or sets the total time allowed for a particular remediation process.

c. Enter the **Retry Count []**. Specifying a retry count sets a limit on the number of times the Agent automatically retries the requirement if it initially fails. (The default retry count setting is 0.)

For details on configuring Auto Remediation, see Configuring Auto Remediation for Requirements, page 9-98.

Note The Cisco NAC Web Agent does not support Auto Remediation.

Step 6 Choose an **Antivirus Product Name** from the dropdown menu or choose **ANY**. The **Products** table lists all the virus definition product versions supported per client OS.

Note Cisco recommends specifying vendor names when appropriate because choosing the **ANY** option can affect the Agent's performance (the process takes longer) on the client machine.

Step 7 For the **Requirement Name,** type a unique name to identify this AV virus definition file requirement in the Agent. The name will be visible to users on the Agent dialogs.

Step 8 In the **Description** field, type a description of the requirement and instructions to guide users who fail to meet the requirement. For an AV Definition Update requirement, you should include instructions to alert Cisco NAC Web Agent users of the requirement and for Cisco NAC Agent users to click the **Update/Remediate** button to update their systems.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 9 Click the checkbox for at least one client **Operating System** (at least one must be chosen).

Step 10 Click **Add Requirement** to add the requirement to the Requirement List.

Figure 9-21 Mac OS X Agent Assessment Report AV Definition Update Requirement Display



Create an AS Rule

Note Your CAM/CAS must be running Cisco NAC Appliance release 4.5 or later and have the latest Cisco AV/AS support updates in order to perform client remediation using version 4.5.0.0+ of the Mac OS X Agent.

Use the following steps to configure an AS rule.

Step 1 Make sure you have the latest version of the Supported AV/AS Product List, as described in Retrieving Cisco NAC Appliance Updates, page 9-12.

Step 2 Go to **Device Management > Clean Access > Clean Access Agent > Rules > New AS Rule**.

Figure 9-22 New AS Rule—Windows

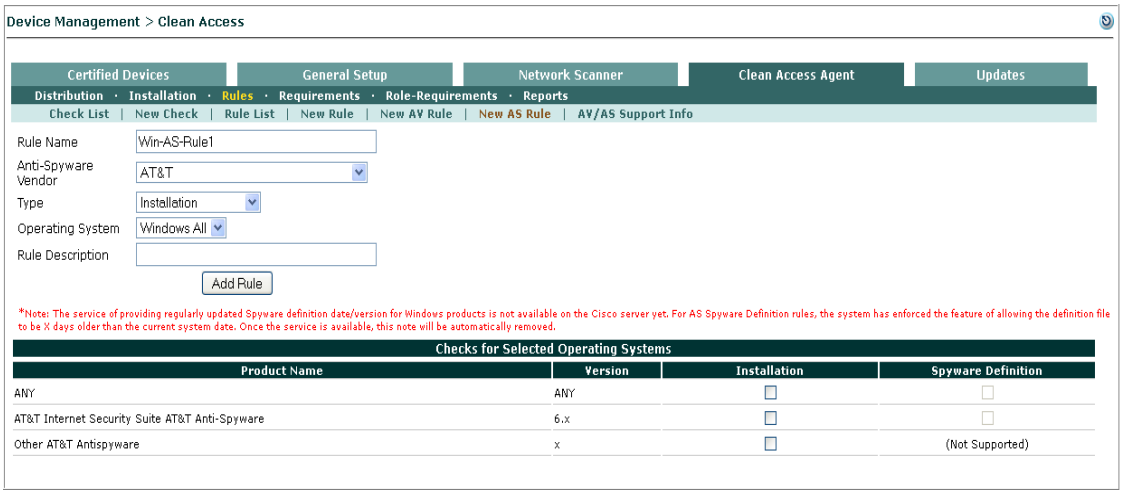
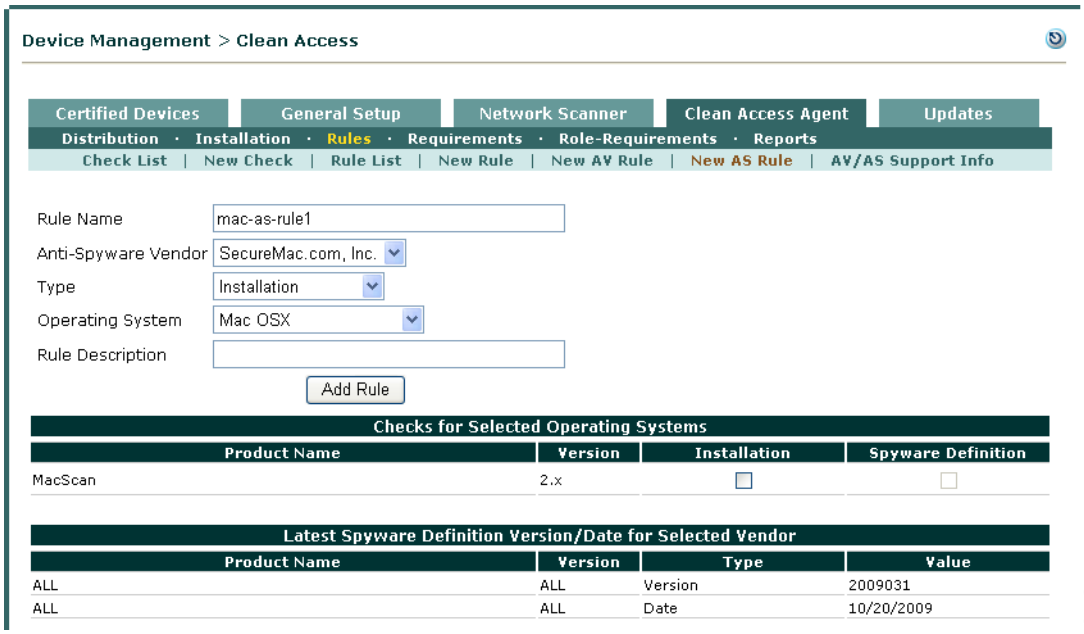

Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Distribution · Installation · Rules · Requirements · Role-Requirements · Reports
Check List | New Check | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info
Rule Name
Win-AS-Rule1
Anti-Spyware Vendor
AT&T
Type
Installation
Operating System
Windows All
Rule Description
Add Rule
*Note: The service of providing regularly updated Spyware definition date/version for Windows products is not available on the Cisco server yet. For AS Spyware Definition rules, the system has enforced the feature of allowing the definition file to be X days older than the current system date. Once the service is available, this note will be automatically removed.
Checks for Selected Operating Systems
Product Name
Version
Installation
Spyware Definition
ANY
ANY
AT&T Internet Security Suite AT&T Anti-Spyware
6.x
Other AT&T Antispyware
x
(Not Supported)
303215

Figure 9-23 New AS Rule—Mac OS X



Step 3 Type a **Rule Name**. You can use digits and underscores, but no spaces in the name.

Step 4 Choose an **Anti Spyware Vendor** from the dropdown menu, or choose **ANY** to select any supported AS vendor or product. This correspondingly populates the **Checks for Selected Operating Systems** table at the bottom of the page with the supported products and product versions from this vendor (for the **Operating System** chosen).

Note Cisco recommends specifying vendor names when appropriate because choosing the **ANY** option can affect the Agent's performance (the process takes longer) on the client machine.

Step 5 From the **Type** dropdown menu, choose either **Installation** or **Spyware Definition**. This enables the checkboxes for the corresponding Installation or Spyware Definition column in the table below.

Step 6 Choose an **Operating System** from the dropdown menu:

- **Windows All**
- **Mac OSX**

Step 7 Type an optional **Rule Description**.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 8 In the **Checks for Selected Operating Systems** table, choose the product versions you want to check for on the client by clicking the checkbox(es) in the corresponding **Installation** or **Spyware Definition** column:

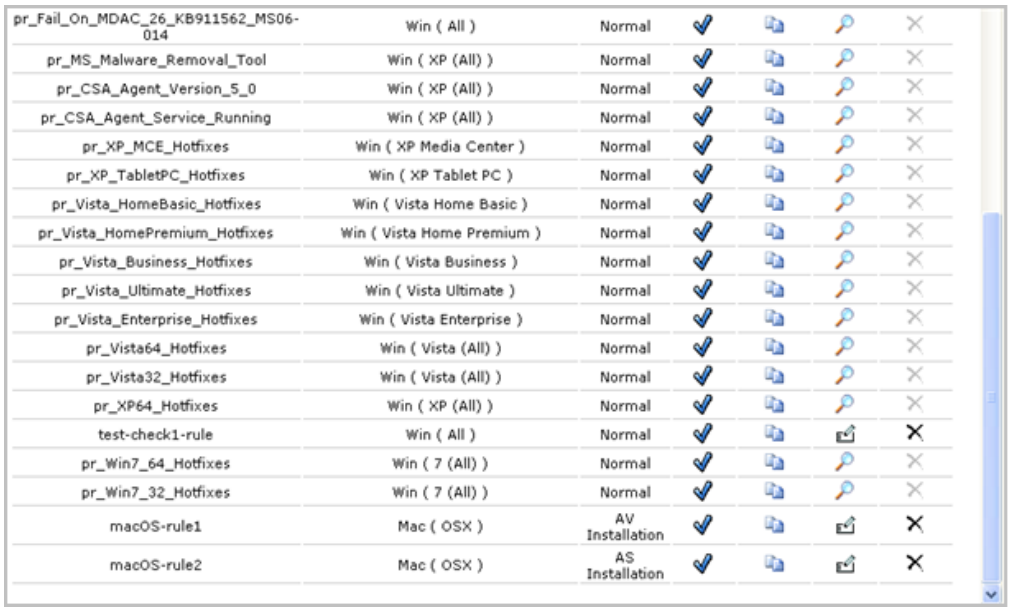
- **ANY** means you want to check for any product and any version from this AS vendor.
- **Installation** checks whether the product is installed,

- **Spyware Definition** checks whether the spyware definition files are up to date on the client for the specified product.

Note In a definition rule, the Agent first confirms whether or not the product is installed, then checks whether or not the definition file is up-to-date.

Step 9 Click **Add Rule**. The new AS rule will be added at the bottom of the **Rule List** with the name you provided (see Figure 9-24).

Figure 9-24 New AS Rules Appear at the Bottom of the Rule List—Mac OS X Example


pr_Fail_On_MDAC_26_KB911562_MS06-014 Win (All) Normal
pr_MS_Malware_Removal_Tool Win (XP (All)) Normal
pr_CSA_Agent_Version_5_0 Win (XP (All)) Normal
pr_CSA_Agent_Service_Running Win (XP (All)) Normal
pr_XP_MCE_Hotfixes Win (XP Media Center) Normal
pr_XP_TabletPC_Hotfixes Win (XP Tablet PC) Normal
pr_Vista_HomeBasic_Hotfixes Win (Vista Home Basic) Normal
pr_Vista_HomePremium_Hotfixes Win (Vista Home Premium) Normal
pr_Vista_Business_Hotfixes Win (Vista Business) Normal
pr_Vista_Ultimate_Hotfixes Win (Vista Ultimate) Normal
pr_Vista_Enterprise_Hotfixes Win (Vista Enterprise) Normal
pr_Vista64_Hotfixes Win (Vista (All)) Normal
pr_Vista32_Hotfixes Win (Vista (All)) Normal
pr_XP64_Hotfixes Win (XP (All)) Normal
test-check1-rule Win (All) Normal
pr_Win7_64_Hotfixes Win (7 (All)) Normal
pr_Win7_32_Hotfixes Win (7 (All)) Normal
macOS-rule1 Mac (OSX) AV Installation
macOS-rule2 Mac (OSX) AS Installation
236835

Create an AS Definition Update Requirement

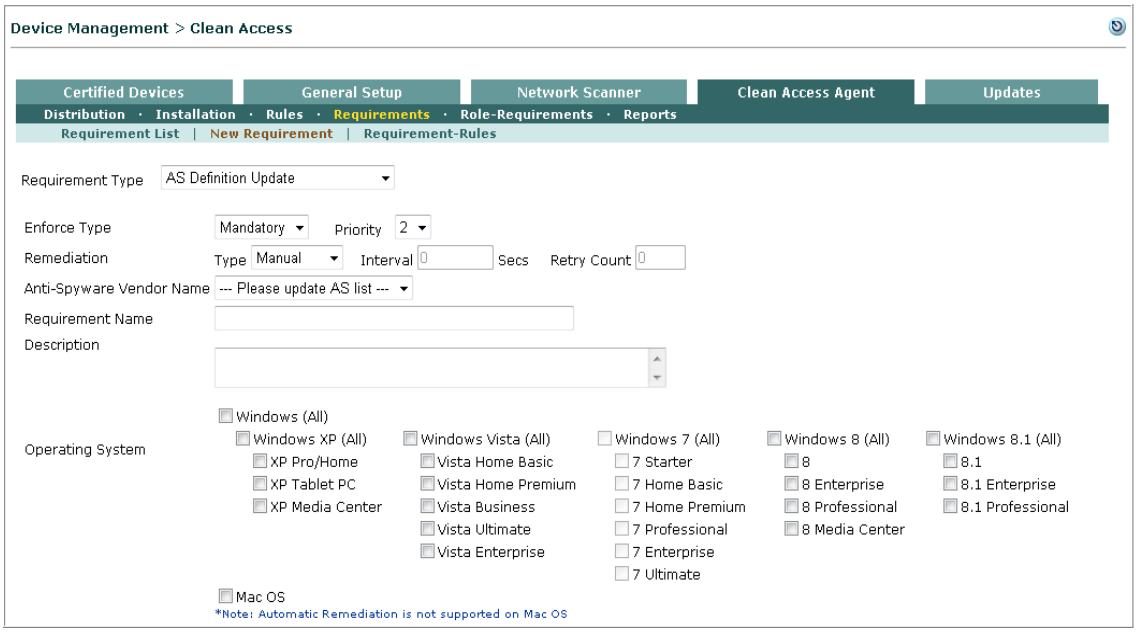
Note Although the Mac OS X Agent supports both AV and AS definition updates, the Compliance Module library currently associated with Cisco NAC Appliance does not contain an AS definition update. Therefore, no AS definition update is currently available on the CAM AS Definition Update requirement configuration page.

For a list of support AV/AS applications, see the "Clean Access Supported AV/AS Product List" section of the corresponding *Release Notes for Cisco NAC Appliance*.

Use the following steps to configure an AS Definition Update requirement.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**.

Figure 9-25 New AS Definition Update Requirement



Step 2 For **Requirement Type** choose **AS Definition Update**

Step 3 Choose an **Enforce Type** from the dropdown menu:

- **Mandatory**—Enforce requirement.The user is informed of this requirement and cannot proceed or have network access unless the client system meets it.
- **Optional**— Do not enforce requirement. The user is informed of the requirement but can bypass it if desired (by clicking **Next/Skip** in the Agent dialog). The client system does not have to meet the requirement for the user to proceed or have network access.
- **Audit**—Silently audit. The client system is checked "silently" for the requirement without notifying the user, and a report is automatically generated and sent back to the CAS. (Audit requirements do not appear in the Mac OS X user's Assessment Report window.) The report results (pass or fail) do not affect user network access.

  Refer to Configuring an Optional/Audit Requirement, page 9-94 for details.

Step 4 Choose the **Priority** of execution for this requirement on the client.

Note The Mac OS X Agent does not support automatic remediation. Therefore, the Remediation functions that appear on the New Requirement configuration page (Remediation **Type**, **Interval**, and **Retry Count**) do not serve any purpose when creating requirement types for Macintosh client remediation.

Step 5 If you want to enable and configure Auto Remediation for the Agent:

a. Choose the **Remediation Type [Manual | Automatic]** from the dropdown menu. Choosing **Manual** preserves previous Agent behavior. The user has to click through each of the requirements using the **Next/Skip** button in the Agent. Choosing **Automatic** sets the Agent to perform Auto Remediation, where the Agent automatically performs updates or launches required programs on the client after the user logs in.

b. If you configure the requirement to use automatic remediation, specify the **Interval** in seconds (the default interval is 0). Depending on the requirement type, this interval either sets the delay before the Agent re-attempts remediation or sets the total time allowed for a particular remediation process.

c. Enter the **Retry Count []**. Specifying a retry count sets a limit on the number of times the Agent automatically retries the requirement if it initially fails. (The default retry count setting is 0.)

For details on configuring Auto Remediation, see Configuring Auto Remediation for Requirements, page 9-98.

Note The Cisco NAC Web Agent does not support Auto Remediation.

Step 6 Choose an **Anti-Spyware Vendor Name** from the dropdown menu or choose **ANY**. The **Products** table lists all the spyware definition product versions currently supported per client OS.

Note Cisco recommends specifying vendor names when appropriate because choosing the **ANY** option can affect the Agent's performance (the process takes longer) on the client machine.

Step 7 For the **Requirement Name,** type a unique name to identify this AS definition file requirement in the Agent. The name will be visible to users on the Agent dialogs.

Step 8 In the **Description** field, type a description of the requirement and instructions to guide users who fail to meet the requirement. For an AS Definition Update requirement, you should include an instruction alerting Cisco NAC Web Agent users of the requirement and for Cisco NAC Agent users to click the **Update/Remediate** button to update their systems.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 9 Click the checkbox for at least one client **Operating System** (at least one must be chosen).

Step 10 Click **Add Requirement** to add the requirement to the Requirement List.

Configuring a Windows Server Update Services Requirement

The Agent "Windows Server Update Services" requirement type allows administrators to launch Windows Server Update Services (WSUS) on Agent user machines based on the following:

- Cisco Rules (e.g. pr_<*Windows operating system*>_hotfixes) and/or administrator-configured custom rules for a specific Windows operating system
- Windows Update severity checks

If you choose to validate Windows client machines using "Cisco Rules," you must also map the WSUS requirement to one or more rules in the CAM. You can choose to map the requirement to existing Cisco (pr_hotfix) rules or to custom rules you create to ensure client machines meet specific criteria before granting access to the Cisco NAC Appliance network. Because external server access is not required,

using Cisco Rules can provide for quicker client validation and user login. However, client machines are only checked against "Critical" hotfixes encompassed by the Cisco Rules. For details on pr_rules, see Configuring Custom Checks, Rules, and Requirements, page 9-70.

If you choose to validate client machines using Windows Update "Severity" options, you do not have to configure requirement-rule mapping and you can choose the level of hotfix to check against. The "Severity" posture assessment settings require access to external WSUS update servers to both verify client machine security compliance and install Windows updates, which can take a significantly longer period of time to complete.

The "Windows Server Update Services" requirement provides an **Update** button on the Agent for remediation. When the end user clicks the **Update** button, the Agent launches the Automatic Updates Agent and forces it to get the update software from a Microsoft-managed or local/third-party-managed WSUS server. You can make the WSUS requirement **Mandatory**, however, the software download from WSUS servers can take some time (particularly if you are using "Severity" settings to validate client machines). Therefore, Cisco recommends making the WSUS requirement "Optional" so that WSUS remediation takes place as a background process on the client machine.

Note The Cisco NAC Web Agent only supports **Go To Link** manual remediation and **File Distribution** functionality. Cisco NAC Web Agent does not support **Update** or **Launch** remediation actions, nor does it perform Auto Remediation.

If you only need to enable or disable Windows Updates (that is, if you do not require specific updates based on the Microsoft severity level), you can configure a standard Windows Update requirement instead of a WSUS requirement. For more information, see Configuring a Windows Update Requirement, page 9-64.

Prerequisites

- The network administrator must ensure the Automatic Updates Agent is updated to support a local WSUS server to support auto-launch capabilities. For details, refer to:
  - http://www.microsoft.com/windowsserversystem/updateservices/evaluation/faqs.mspx
- The "Windows Server Update Services" requirement type is only for Windows 8.1/8/7/XP/Vista.
- In order to support Windows Server Update Services operations, client machines must have version 5.4.3790.1000 (or a more recent version) of the WUAUENG.dll file installed.
- If users without Administrator privileges are using WSUS to update Windows, you must choose the **No UI** option for the **Installation Wizard Interface Setting** when configuring a WSUS requirement.
- Some Microsoft Windows components (i.e., Internet Explorer 7) require admin privileges in order to successfully update. If the user does not have admin privileges on the client machine, the Windows update process returns a "WU_E_NO_INTERACTIVE_USER" error. Therefore, Cisco recommends making any Windows updates requiring admin privileges "Optional" to minimize update failures. For details, refer to http://msdn2.microsoft.com/en-us/library/aa387289.aspx.
- WSUS forced updates can take a while. They are launched and run in the background.
- If there are update errors, refer to **C:\Windows\Windows Update.log** or **C:\Windows\WindowsUpdate.log** on the client machine.

The steps to create a Windows Server Update Service Requirements are:

Step 1 Create Windows Server Update Service Requirement, page 9-59

Step 2 Map Windows Server Update Service Requirement to Windows Rules, page 9-63

Step 3 Apply Requirements to User Roles, page 9-92

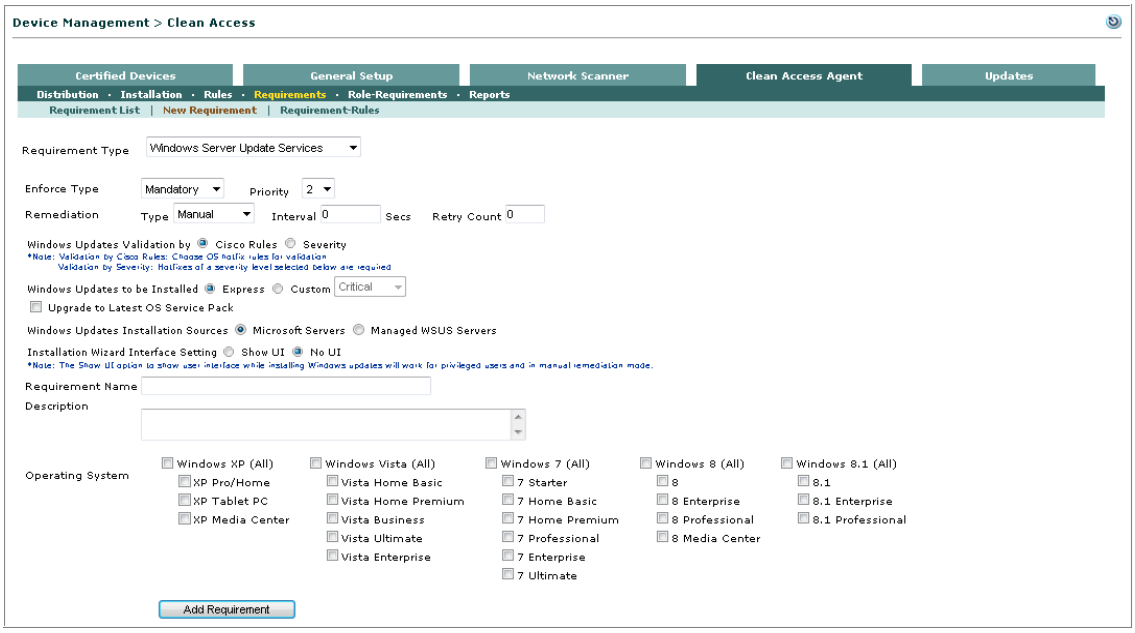
Step 4 Validate Requirements, page 9-93

Create Windows Server Update Service Requirement

Use the following steps to configure a Windows Server Update Service (WSUS) requirement.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**.

Figure 9-26 New Windows Server Update Service Requirement



Step 2 From the **Requirement Type** dropdown menu, choose **Windows Server Update Services**.

Step 3 Choose an **Enforce Type** from the dropdown menu:

- **Mandatory**—Enforce requirement.The user is informed of this requirement and cannot proceed or have network access unless the client system meets it.
- **Optional**— Do not enforce requirement. The user is informed of the requirement but can bypass it if desired (by clicking **Next/Skip** in the Agent dialog). The client system does not have to meet the requirement for the user to proceed or have network access.
- **Audit**—Silently audit. The client system is checked "silently" for the requirement without notifying the user, and a report is generated. The report results (pass or fail) do not affect user network access.

  Refer to Configuring an Optional/Audit Requirement, page 9-94 for details.

Step 4 Choose the **Priority** of execution for this requirement on the client. A high priority (e.g. 1) means this requirement is checked on the system ahead of all other requirements (and appears in the Agent dialogs in that order). Note that if this is a Mandatory requirement and it fails, the Agent does not continue past that point until that requirement succeeds.

Step 5 If you want to enable and configure Auto Remediation for the Agent:

a. Choose the **Remediation Type [Manual | Automatic]** from the dropdown menu. Choosing **Manual** preserves previous Agent behavior. The user has to click through each of the requirements using the **Next/Skip** button in the Agent. Choosing **Automatic** sets the Agent to perform Auto Remediation, where the Agent automatically performs updates or launches required programs on the client after the user logs in.

b. If you configure the requirement to use automatic remediation, specify the **Interval** in seconds (the default interval is 0). Depending on the requirement type, this interval either sets the delay before the Agent re-attempts remediation or sets the total time allowed for a particular remediation process.

c. Enter the **Retry Count []**. Specifying a retry count sets a limit on the number of times the Agent automatically retries the requirement if it initially fails. (The default retry count setting is 0.)

For details on configuring Auto Remediation, see Configuring Auto Remediation for Requirements, page 9-98.



Note The Cisco NAC Web Agent does not support Auto Remediation.

Step 6 Under **Windows Updates Validation by**, specify the validation method to use when checking the Windows operating system installed on the client machine:

- **Cisco Rules**—Use Cisco Rules (e.g. pr_<*Windows operating system*>_Hotfixes) or similar administrator-configured custom rules on the CAM to verify whether the client Windows operating system meets minimum security standards. This is the faster method to assess the client machine's security posture, as it relies on criteria available in the CAM's local database. For fastest execution, Cisco recommends using Cisco Rules as the validation method with **Express** installation (which installs "Critical and Important" Windows updates) and **Windows Servers** as the installation source.



Note If you choose this option, you also need to configure requirement-rule mapping, as described in Map Windows Server Update Service Requirement to Windows Rules, page 9-63.

If you wish to validate against your own custom rules, Cisco recommends that you configure them similarly to an existing Cisco Rule (e.g pr_<*Windows operating system*>_Hotfixes). You should know the level of severity of the hotfix to check for (e.g. "Important" vs. "Low"). Refer to Copying Checks and Rules, page 9-72 for details.

- **Severity**—Verify whether or not the Windows operating system on the client meets minimum security standards using a Microsoft-managed or local Windows Update server. With this validation method, you do not need to map the WSUS requirement to any rules. However, the **Severity** setting requires the CAM to use an external WSUS server to verify updates currently installed on the client machine and then install the Windows updates necessary to meet the requirement.

When you use locally-managed or hosted Windows (WSUS) servers to perform the Windows updates to satisfy a WSUS requirement, the Agent calls on WSUS to install the updates. Note that the WSUS Agent automatically installs *all* of the updates available for the specified severity level. (That is, if there are 5 "Important" updates and 3 "Critical" updates and the client machine already

features some of the updates, the WSUS installer still automatically installs *all* of the updates specified by the requirement type.) As a result, validating client matches based on severity can take a longer period of time to assess and remediate.

Note You set the validation method to coincide with the **Severity** option using the **Windows Updates Installation Sources** setting in step 9.

Step 7 Under **Windows Updates to be Installed**, specify the level of updates to install. The validation method essentially checks what's missing on the machine to trigger an update. The actual update will originate from Microsoft or WSUS servers. The number of updates installed depends on the level of updates you choose here. For example, if you choose validation by Cisco Rules, which only checks for Critical hotfixes, but choose **Custom** Windows Updates to be Installed, with a level of **Medium**, all "Critical, Important, and Moderate" hotfixes will be installed on the client, but only if the client is missing Critical hotfixes to begin with.

- **Express**—This option installs the same Windows updates as would be available from the Windows Update application "Express" option. Typically, the "Express" option includes only the "Important and Critical" Windows updates. However, if the Microsoft version of the Express update includes other installations (like a Service Pack update, for example), then *all* of the updates are automatically installed on the client machine.
- **Custom**—Use this setting and the associated dropdown menu to install updates based on their severity by choosing **Critical**, **Medium**, or **All** from the associated dropdown menu.
  - **Critical**—Installs only "Critical" Microsoft Windows updates.
  - **Medium**—Installs all "Critical, Important, and Moderate" Windows updates.
  - **All**—Installs all "Critical, Important, Moderate, and Low" Windows updates.

  In all cases, the WSUS server automatically downloads *all* of the updates to install on the client. Therefore, even if the client machine already features 3 of 5 updates of a given severity, the WSUS server still downloads and installs all updates.

Step 8 Click **Upgrade to Latest OS Service Pack** to automatically install the latest service pack available for the user's operating system.

Note This option is automatically included in the install process when you specify either **Medium** or **All** Custom updates, above, and cannot be "left out." If you specified **Critical** Custom updates, you can choose to enable or disable this option.

Cisco Rules validate all "Critical" Windows updates and verify whether or not minimum Windows XP Service Pack updates are installed on the client machine. If you choose to require only "Critical" **Windows Updates to be Installed**, Windows XP Service Pack 2 may not be present on the client machine, hence, the client machine will not pass posture assessment via "Cisco Rules." To address this potential problem, Cisco recommends that if you choose to validate client machines using "Cisco Rules" and require only "Critical" updates, that you also require Service Pack Updates to ensure any clients validated using "Cisco Rules" pass posture assessment. (If you choose to validate client machines according to "Severity" rather than "Cisco Rules," this is not an issue.)

Note Windows Service Pack updates traditionally take a long time to download and install. Before you require users to update their Windows operating system with a full service pack installation, be sure you extend the session timeout period for Temporary Role users to accommodate the long install and update process. (See Configure Session Timeout for the Temporary Role, page 8-19.)

Step 9 For **Windows Updates Installation Sources**, specify the source for the Windows update(s):

- **Windows Servers**—Updates the Windows operating system using Microsoft-managed Windows update servers.
- **Managed WSUS Servers**—Updates the Windows operating system using resources managed by the Windows server administrator or other trusted third-party source.

Step 10 For **Installation Wizard Interface Setting**, specify whether or not the user sees the Installation Wizard user interface during Windows Update installation:

- **Show UI**—The Windows Update Installation Wizard progress is visible to users during the update process so they can tell what components are being updated and when the update completes. (Users must have Administrator privileges on the client machine in order to see the Installation Wizard user interface during Windows Update.)
- **No UI**—The Windows Update takes place in the background once the update process has begun and the user is only notified when the update is complete.

Note

- If users without Administrator privileges are using WSUS to update Windows, you must choose the **No UI** option.
- When a WSUS update is performed on a new installation of Windows 7 (where no updates have been applied), and the **No UI** option is selected for the requirement, the WSUS update can fail.

  The portion of the Windows update that fails to install is the KB890830 update (Windows Malicious Software Removal Tool, http://support.microsoft.com/?kbid=890830). This upgrade must be installed with admin privileges and there is a one time EULA that the user must accept during installation.

  After KB890830 is installed, there are monthly updates that are pushed out from Microsoft on patch Tuesday. The subsequent updates of KB890830 do not require admin privileges and they work fine on a client where the user is not a member of the admin group.

  If users manually install KB890830 on a client system as a non-admin user using Windows Update, they are prompted for the administrator password and then get the EULA.

Step 11 For the **Requirement Name**, type a unique name to identify this requirement in the Agent. The name will be visible to users on the Agent dialogs.

Step 12 In the **Description** field, type a description of the requirement and instructions to guide users who fail to meet the requirement, including instructions for Agent users to click the **Update** button to update their systems. Note that **Windows Server Update Service** displays the **Update** button on the Agent.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 13 Click one or more of the following checkboxes to set the **Operating System**(s) for the requirement:

- **Windows XP (All)** or one or more of the specific Windows XP operating systems
- **Windows Vista (All)** or one or more of the specific Windows Vista operating systems
- **Windows 7 (All)** or one or more of the specific Windows 7 operating systems
- **Windows 8(All)** or one or more of the specific Windows 8 operating systems
- **Windows 8.1(All)** or one or more of the specific Windows 8.1 operating systems

Step 14 Click **Add Requirement**.

Step 15 If you configured the WSUS requirement for "Windows Updates Validation by Cisco Rules," continue to the next step, Map Windows Server Update Service Requirement to Windows Rules.

Otherwise, continue to the next steps to complete the configuration:

- Apply Requirements to User Roles, page 9-92
- Validate Requirements, page 9-93

Map Windows Server Update Service Requirement to Windows Rules

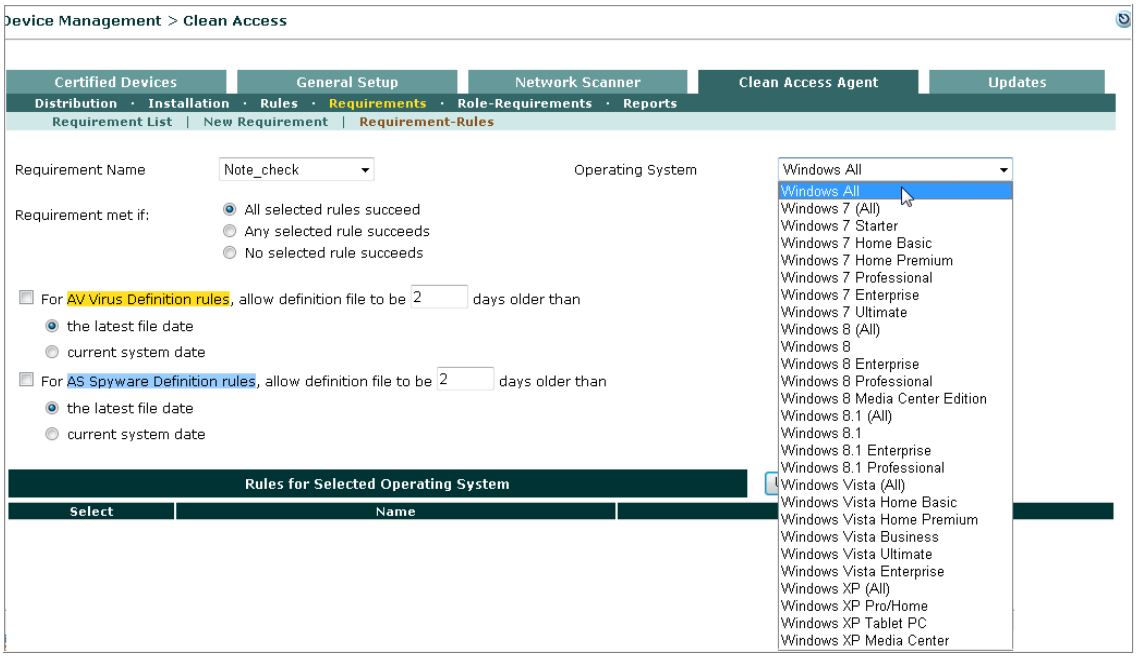
Perform the steps in this section if you configured a Windows Server Update Service requirement for **Windows Updates Validation by Cisco Rules**. (See Create Windows Server Update Service Requirement, page 9-59.)

If you specified **Windows Updates Validation by Severity**, you do not need to map the Windows Server Update Service to an existing Windows Rule and you can skip this section.

Use the following steps to map a Windows Server Update Service requirement to a Windows rule.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**.

Figure 9-27 Map Windows Server Update Service Requirement to Rules



Step 2 From the **Requirement Name** dropdown menu, choose the Windows Server Update Service (WSUS) requirement you configured.

Step 3 To configure the Windows Server Update Service requirement-rule mapping, repeat the following procedure for each operating system you want to validate for this requirement:

a. In the **Operating System** dropdown menu, choose one of the operating systems you configured for the requirement in step 13 of Configuring a Windows Server Update Services Requirement, page 9-57.

Rules are categorized in the system according to the operating system for which they are configured. The **Operating System** dropdown determines which Rules appear for selection in the "Rules for Selected Operating System" table at the bottom of the page. For example, if you want to map multiple hotfix rules to a requirement you configured for Windows XP (All), in the Requirement-Rule page, you must individually select each flavor of Windows XP (e.g.Windows XP Pro/Home, Windows XP Tablet PC, Windows XP Media Center) from the Operating System

dropdown to be able to view and select the pr_hotfix rules for each of those OS flavors (e.g. pr_XP_Hotfixes, pr_XP_TabletPC_Hotfixes, and pr_XP_MCE_Hotfixes, respectively) in the "Rules for Selected Operating System" list.

b. Choose one of the following options for **Requirement met if**:

- **All selected rules succeed** (default)—all the rules must be satisfied for the client to be considered in compliance with the requirement.
- **Any selected rule succeeds**—at least one selected rule must be satisfied for the client to be considered in compliance with the requirement.
- **No selected rule succeeds**—the selected rules must all fail for the client to be considered in compliance with the requirement.

c. Ignore the AV Virus/AS Spyware Definition rule options.

d. The **Rules for Selected Operating System list** will display all rules that exist in the system for the chosen OS (pr_ rules or rules that you have configured). Click the checkbox for each rule you want to enable for this requirement. Rules that are typically associated to this requirement are:

- pr_AutoUpdateCheck_Rule (Windows XP (All)
- pr_XP_Hotfixes (Windows XP Pro/Home)
- pr_Vista_<*version*>_Hotfixes (Windows Vista Home Basic/Premium, Business, Ultimate, Enterprise)

Note that all rules are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Rule List**.

e. Click **Update** to complete the mapping.

Step 4 Continue to the next steps—Apply Requirements to User Roles, page 9-92 and Validate Requirements, page 9-93—to complete the configuration.

Configuring a Windows Update Requirement

The Agent "Windows Update" Requirement type configuration page allows administrators to check and modify Windows Update settings, and launch Windows Updater on client machines where users have Administrator privileges.

When this requirement is configured, the administrator can turn on Automatic Updates on Windows Vista or Windows XP client machines which have this option disabled on the machine.

The Windows Update requirement (set to Optional by default) provides an **Update** button on the (persistent) Agent for remediation. When the end user clicks the **Update** button, the Agent launches the Automatic Updates Agent and forces it to get the update software from an external WSUS server. The software download from the WSUS server may take some time. Therefore, Cisco recommends you keep the Windows Update requirement Optional so that remediation occurs in the background.



Note The Cisco NAC Web Agent only supports **Go To Link** manual remediation and **File Distribution** functionality. Cisco NAC Web Agent does not support **Update** or **Launch** remediation actions, nor does it perform Auto Remediation.

Windows operating systems can be customized in many ways to include hotfixes and service packs as part of the operating system installation. In some cases, the Agent may not be able to detect hotfix key values in the registry when the hotfix is part of the operating system. In these cases, Cisco recommends using the Windows Server Update Services (WSUS) requirement, which can be configured to access external Windows Updates servers. For more information, see Configuring a Windows Server Update Services Requirement, page 9-57.

Prerequisites

- The Windows Server Update Services requirement type applies only to Windows 8.1/8/7/Vista/XP client machines. It supports checking Cisco- and Windows-based client operating system verification and customized update installation options based on update severity.
- The network administrator must ensure the Automatic Updates Agent is updated to support a local WSUS server to support auto-launch capabilities. For details, refer to http://www.microsoft.com/windowsserversystem/updateservices/evaluation/faqs.mspx
- In order to support Windows Server Update Services operations, client machines must have version 5.4.3790.1000 (or a more recent version) of the WUAUENG.dll file installed.
- WSUS forced update may take a while. Generally, it is launched and run in the background.
- Some Microsoft Windows components (such as Internet Explorer 7) require admin privileges in order to successfully update. If the user does not have admin privileges on the client machine, the Windows update process returns a “WU_E_NO_INTERACTIVE_USER” error. Therefore, Cisco recommends making any Windows updates requiring admin privileges “Optional” to minimize update failures. For details, refer to http://msdn2.microsoft.com/en-us/library/aa387289.aspx.
- If there are update errors, see C:\Windows\Windows Update.log or C:\Windows\WindowsUpdate.log.

The steps to configure a Windows Update requirements are as follows:

Step 1 Create a Windows Update Requirement, page 9-66

Step 2 Map Windows Update Requirement to Windows Rules, page 9-69

Step 3 Apply Requirements to User Roles, page 9-92

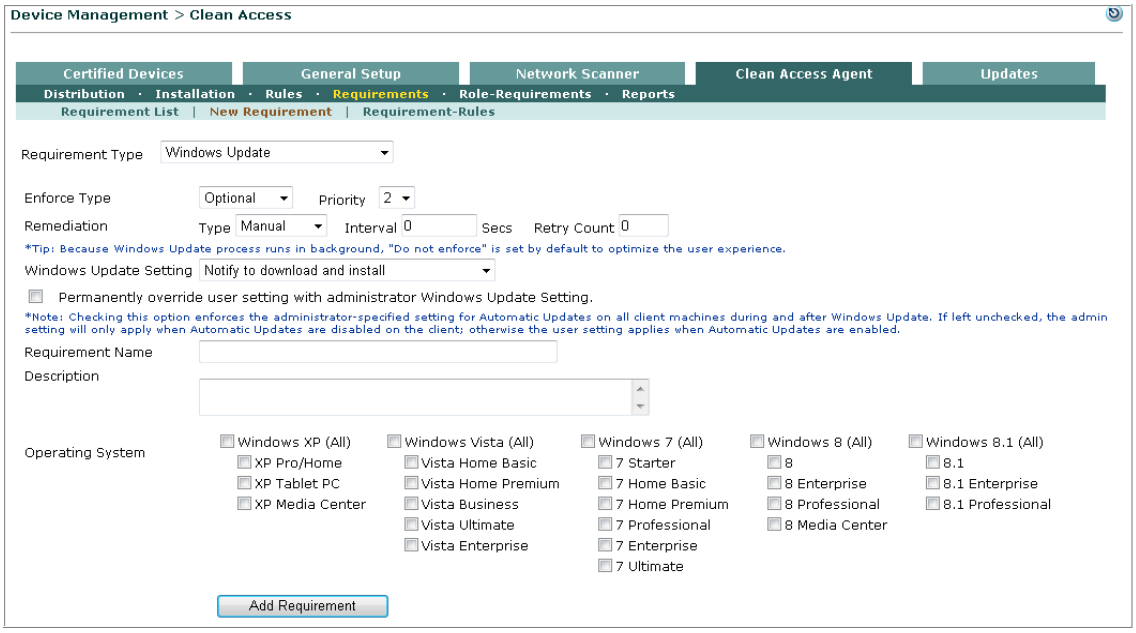
Step 4 Validate Requirements, page 9-93

Create a Windows Update Requirement

Use the following steps to configure a Windows Update requirement.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**.

Figure 9-28 New Windows Update Requirement



Step 2 From the **Requirement Type** dropdown menu, choose **Windows Update**.

Step 3 Choose an **Enforce Type** from the dropdown menu:

- **Optional** (default setting)—Do not enforce requirement. The user is informed of the requirement but can bypass it if desired (by clicking **Next/Skip** in the Agent dialog). The client system does not have to meet the requirement for the user to proceed or have network access.

  Note The Windows Update requirement type is set to **Optional** (or "do not enforce") by default to optimize user experience by running the update process in the background. Cisco also recommends leaving this requirement as Optional if selecting the "Automatically download and install" option.

- **Mandatory**—Enforce requirement.The user is informed of this requirement and cannot proceed or have network access unless the client system meets it.
- **Audit**—Silently audit. The client system is checked "silently" for the requirement without notifying the user, and a report is generated. The report results (pass or fail) do not affect user network access.

  Refer to Configuring an Optional/Audit Requirement, page 9-94 for details.

Step 4 Choose the **Priority** of execution for this requirement on the client. A high priority (e.g. 1) means this requirement is checked on the system ahead of all other requirements (and appears in the Agent dialogs in that order). Note that if this is a Mandatory requirement and it fails, the Agent does not continue past that point until that requirement succeeds.

Step 5 If you want to enable and configure Auto Remediation for the Agent:

a. Choose the **Remediation Type [Manual | Automatic]** from the dropdown menu. Choosing **Manual** preserves previous Agent behavior. The user has to click through each of the requirements using the **Next/Skip** button in the Agent. Choosing **Automatic** sets the Agent to perform Auto Remediation, where the Agent automatically performs updates or launches required programs on the client after the user logs in.

b. If you configure the requirement to use automatic remediation, specify the **Interval** in seconds (the default interval is 0). Depending on the requirement type, this interval either sets the delay before the Agent re-attempts remediation or sets the total time allowed for a particular remediation process.

c. Enter the **Retry Count []**. Specifying a retry count sets a limit on the number of times the Agent automatically retries the requirement if it initially fails. (The default retry count setting is 0.)

For details on configuring Auto Remediation, see Configuring Auto Remediation for Requirements, page 9-98.

Note The Cisco NAC Web Agent does not support Auto Remediation.

Step 6 From the **Windows Update Setting** dropdown, choose one of the following options:

- **Do not change setting**
- **Notify to download and install**
- **Automatically download and notify to install**
- **Automatically download and install**

These settings correspond to the **Automatic Updates** dialog settings on the Windows client (Figure 9-29)

Step 7 Click the checkbox for **Permanently override user setting with administrator Windows Update Setting**, if you want to enforce your administrator-specified setting for Automatic Updates on all client machines during and after Windows Update. If left unchecked, the admin setting will only apply when Automatic Updates are disabled on the client; otherwise the user setting applies when Automatic Updates are enabled.

Step 8 For the **Requirement Name**, type a unique name to identify this requirement in the Agent. The name will be visible to users on the Agent dialogs.

Step 9 In the **Description** field, type a description of the requirement and instructions to guide users who fail to meet the requirement, including instructions for Agent users to click the **Update** button to update their systems. Note that **Windows Update** displays the **Update** button on the Agent.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 10 Click one or more of the following checkboxes to set the **Operating System**(s) for the requirement:

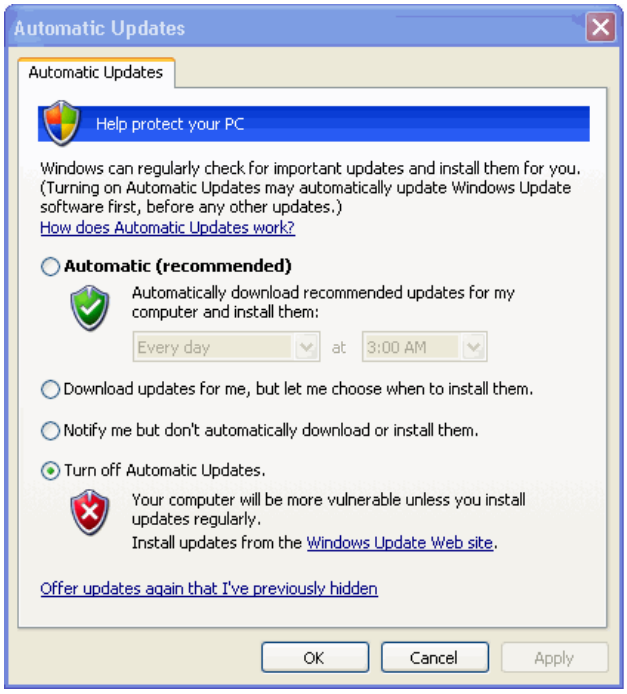
- **Windows XP (All)** or one or more of the specific Windows XP operating systems

- **Windows Vista (All)** or one or more of the specific Windows Vista operating systems
- **Windows 7 (All)** or one or more of the specific Windows 7 operating systems
- **Windows 8 (All)** or one or more of the specific Windows 8 operating systems
- **Windows 8.1 (All)** or one or more of the specific Windows 8.1 operating systems

Note Make sure the operating system you choose matches the operating system you set for the rule(s) you plan to map to this Windows Update requirement in Configuring a Windows Server Update Services Requirement, page 9-57.

Step 11 Click **Add Requirement**.

Figure 9-29 Windows XP Automatic Updates

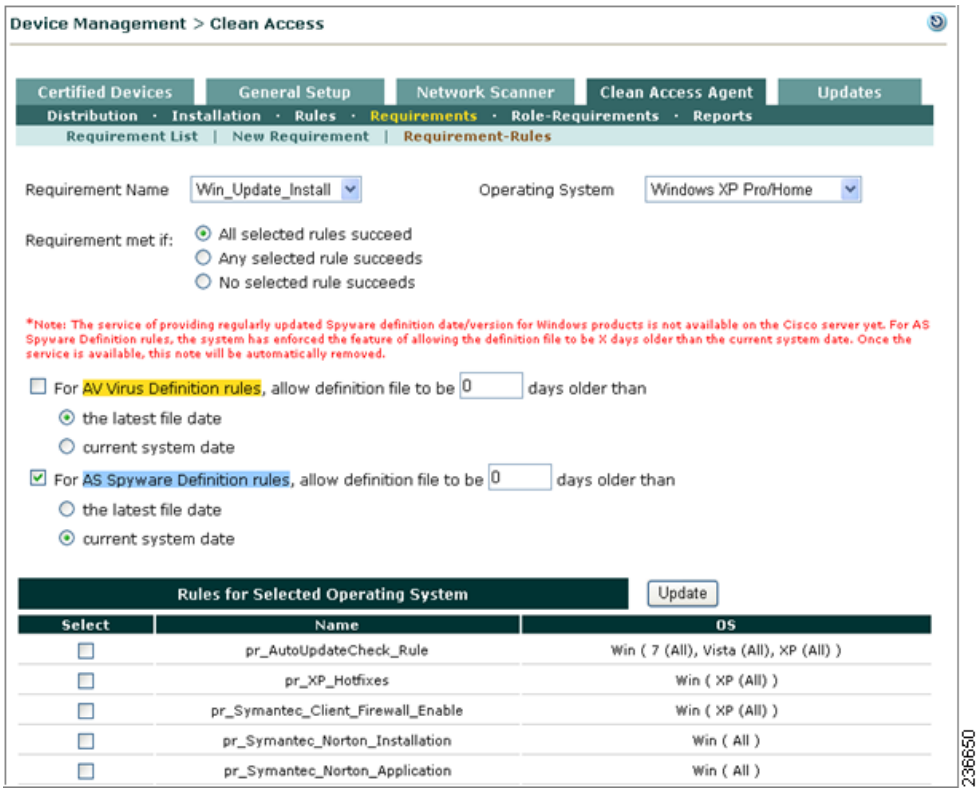

Automatic Updates
Automatic Updates
Help protect your PC
Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)
How does Automatic Updates work?
Automatic (recommended)
Automatically download recommended updates for my computer and install them:
Every day
at
3:00 AM
Download updates for me, but let me choose when to install them.
Notify me but don't automatically download or install them.
Turn off Automatic Updates.
Your computer will be more vulnerable unless you install updates regularly.
Install updates from the Windows Update Web site.
Offer updates again that I've previously hidden
OK
Cancel
Apply
183516

Map Windows Update Requirement to Windows Rules

Use the following steps to map a Windows Update requirement to one or more rules.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**.

Figure 9-30 Map Windows Update Requirement to Rules


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Distribution · Installation · Rules · Requirements · Role-Requirements · Reports
Requirement List | New Requirement | Requirement-Rules
Requirement Name
Win_Update_Install
Operating System
Windows XP Pro/Home
Requirement met if:
All selected rules succeed
Any selected rule succeeds
No selected rule succeeds
*Note: The service of providing regularly updated Spyware definition date/version for Windows products is not available on the Cisco server yet. For AS Spyware Definition rules, the system has enforced the feature of allowing the definition file to be X days older than the current system date. Once the service is available, this note will be automatically removed.
For AV Virus Definition rules, allow definition file to be 0 days older than
the latest file date
current system date
For AS Spyware Definition rules, allow definition file to be 0 days older than
the latest file date
current system date
Rules for Selected Operating System
Update
Select
Name
OS
pr_AutoUpdateCheck_Rule
Win (7 (All), Vista (All), XP (All))
pr_XP_Hotfixes
Win (XP (All))
pr_Symantec_Client_Firewall_Enable
Win (XP (All))
pr_Symantec_Norton_Installation
Win (All)
pr_Symantec_Norton_Application
Win (All)
236650

Step 2 From the **Requirement Name** dropdown menu, choose the Windows Update requirement you configured.

Step 3 To configure the Windows Update requirement-rule mapping, repeat the following procedure for each operating system you want to support:

a. In the **Operating System** dropdown menu, choose one of the operating systems you configured for the requirement in step 10 of Configuring a Windows Update Requirement, page 9-64.

Rules are categorized in the system according to the operating system for which they are configured. The **Operating System** dropdown determines which Rules appear for selection in the "Rules for Selected Operating System" table at the bottom of the page. For example, if you want to map multiple hotfix rules to a requirement you configured for Windows XP (All), in the Requirement-Rule page, you must individually select each flavor of Windows XP (e.g.Windows XP Pro/Home, Windows XP Tablet PC, Windows XPMedia Center) from the Operating System dropdown to be able to view and select the pr_hotfix rules for each of those OS flavors (e.g. pr_XP_Hotfixes, pr_XP_TabletPC_Hotfixes, and pr_XP_MCE_Hotfixes, respectively) in the "Rules for Selected Operating System" list.

b. Choose one of the following options for **Requirement met if**:

- **All selected rules succeed** (default)—all the rules must be satisfied for the client to be considered in compliance with the requirement.
- **Any selected rule succeeds**—at least one selected rule must be satisfied for the client to be considered in compliance with the requirement.
- **No selected rule succeeds**—the selected rules must all fail for the client to be considered in compliance with the requirement.

c. Ignore the AV Virus/AS Spyware Definition rule options.

d. The **Rules for Selected Operating System list** will display all rules that exist in the system for the chosen OS (pr_ rules or rules that you have configured). Click the checkbox for each rule you want to enable for this requirement. Typical rules that are associated to this requirement are:

- pr_AutoUpdateCheck_Rule (Windows XP (All)
- pr_XP_Hotfixes (Windows XP Pro/Home)
- pr_Vista_<*version*>_Hotfixes (Windows Vista Home Basic/Premium, Business, Ultimate, Enterprise)

Note that all rules are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Rule List**.

e. Click **Update** to complete the mapping.

Step 4 Continue to the next steps—Apply Requirements to User Roles, page 9-92 and Validate Requirements, page 9-93—to complete the configuration.

Configuring Custom Checks, Rules, and Requirements

A check is a condition statement used to examine the client system. In the simplest case, a requirement can be created from a single rule made up of a single check. If the condition statement yields a true result, the system is considered in compliance with the Agent requirement and no remediation is necessary.

To create a check, first determine an identifying feature of the requirement. The feature (such as a registry key or process name) should indicate whether the client meets the requirement. The best way to find such an indicator is to examine a system that meets the requirement. If necessary, refer to the documentation provided with the software to determine what identifying feature to use for the Clean Access check. Once you have determined the indicator for the requirement, use the following procedure to create the check.

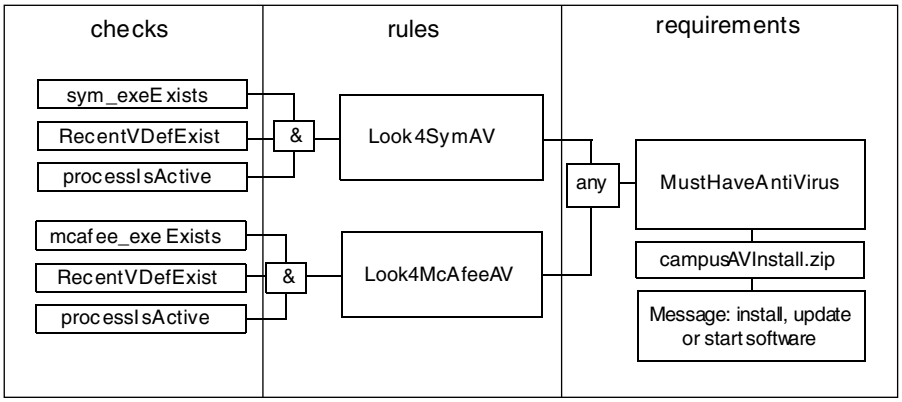
Note The Mac OS X Agent does not support custom checks and custom rules. You can only assign AV and AS rules to the Link Distribution, Local Check, AV Definition Update, and AS Definition Update requirement types for Mac OS X posture remediation.

Custom Requirements

You can create custom requirements to map rules to the mechanism that allows users to meet the rule condition. The mechanism may be an installation file, a link to an external resource, or simply instructions. If a rule check is not satisfied (for example, required software is *not* found on the client system), users can be warned or required to fix their systems, depending on your configuration. As

shown in Figure 9-31, a rule can combine several checks with Boolean operators, "&" (and), "|" (or), and "!" (not). A requirement can rely on more than one rule, specifying that any selected rule, all rules, or no rule must be satisfied for the client to be considered in compliance with the requirement.

Figure 9-31 Custom Checks, Rules, and Requirements



Custom Rules

A rule is a condition statement made up of one or more checks. A rule combines checks with logical operators to form a Boolean statement that can test multiple features of the client system.

Cisco Pre-Configured Rules ("pr_")

Cisco NAC Appliance provides a set of pre-configured rules and checks that are downloaded to the CAM via the **Updates** page on the CAM web console (under **Device Management > Clean Access > Updates**).

Pre-configured rules have a prefix of "pr" in their names (e.g. "pr_XP_Hotfixes"), and can be copied for use as a template, but cannot be edited or removed. You can click the **Edit** icon for any "pr_" rule to view the rule expression that defines it. The rule expression for a pre-configured rule will be composed of pre-configured checks (e.g. "pc_Hotfix835732") and boolean operators. The rule expressions for pre-configured rules are updated via Cisco Updates. For example, when new Critical Windows OS hotfixes are released for Windows XP, the pr_XP_Hotfixes rule will be updated with the corresponding hotfix checks.

Pre-configured rules are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Rule List**.

Note Cisco pre-configured rules are intended to provide support for Critical Windows operating system hotfixes only.

Custom Checks

A check is a condition statement that examines a feature of the client system, such as a file, registry key, service, or application. Table 9-14 lists the types of custom checks available and what they test.

Table 9-14 Checks

Check Category	Check Type
Registry check	• whether or not a registry key exists • registry key value, version, or modification date
File Check	• whether or not a file exists • date of modification or creation • file version
Service check	• whether or not a service is running
Application check	• whether or not an application is running

Cisco Pre-Configured Checks ("pc_")

Pre-configured checks have a prefix of "pc" in their names (for example, pc_Hotfix828035) and are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Check List**.

Using Pre-Configured Rules to Check for CSA

You can use Cisco pre-configured rules to create an Agent requirement that checks if the Cisco Security Agent (CSA) is already installed and/or running on a client. To do this:

1. Create a new Link Distribution or File Distribution requirement (for Windows 8.1/8/7/Vista/XP).
2. Associate the requirement to one or both of the following rules (for Windows 8.1/8/7/Vista/XP):
   - pr_CSA_Agent_Version_5_0
   - pr_CSA_Agent_Service_Running
3. Associate the requirement to the user role(s) for which it will apply.

Note See Configuration Summary, page 9-73 for further details on creating custom requirements (using either pre-configured or custom rules).

Copying Checks and Rules

Note that pre-configured rules and checks are not editable, but can serve as templates. To modify a non-editable check or a rule, make a copy of it first by clicking the corresponding **Copy** icon. Copies of checks are added to the bottom of the **Check List**, in the form `copy_of_checkname`. Copies of rules are added to the bottom of the **Rules List**, in the form `copy_of_rulename`. Click the corresponding **Edit** icon to bring up the Edit form to modify the check or rule. The edited checks and rules can then be configured and associated to requirements and roles as described in the following sections.

Configuration Summary

The steps to create custom requirements are as follows:

Step 1 Create Custom Check, page 9-73

Step 2 Create a Custom Rule, page 9-77

Step 3 Validate Rules, page 9-79

Step 4 Create a Custom Requirement, page 9-80

Step 5 Map Requirements to Rules, page 9-90

Step 6 Apply Requirements to User Roles, page 9-92

Step 7 Validate Requirements, page 9-93

Create Custom Check

Use the following steps to configure a custom Check.

Step 1 In the **Clean Access Agent** tab, click the **Rules** submenu and then open the **New Check** page.

Note For all custom checks, follow steps 2 through 7, refer to the specific configuration settings for each check type, then go to step 8.

Step 2 Select a **Check Category**: **Registry Check**, **File Check**, **Service Check**, or **Application Check**.

Step 3 Select a **Check Type** for the Category and fill in specific form fields as described in the following section. Specify the parameters, operator, and (if the check type is a value comparison) the value and data type of the statement, and click **Add Check** to create the evaluation statement. If the condition statement evaluates to false, the required software is considered missing.

- Registry Checks, page 9-74
- File Checks, page 9-75
- Service Check, page 9-76
- Application Check, page 9-77

Step 4 Type a descriptive **Check Name**. The rules created from this check will reference the check by this name, so be sure to give the check a unique, self-descriptive name. The name is case-sensitive and should be less than 255 characters and without spaces or special characters.

Step 5 Type an optional **Check Description**.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 6 Click one or more of the following checkboxes to set the **Operating System**(s) for the requirement:

- **Windows All**

- **Windows XP (All)** or one or more of the specific **Windows XP** operating systems
- **Windows Vista (All)** or one or more of the specific **Windows Vista** operating systems
- **Windows 7 (All)** or one or more of the specific **Windows 7** operating systems
- **Windows 8 (All)** or one or more of the specific **Windows 8** operating systems
- **Windows 8.1 (All)** or one or more of the specific **Windows 8.1** operating systems

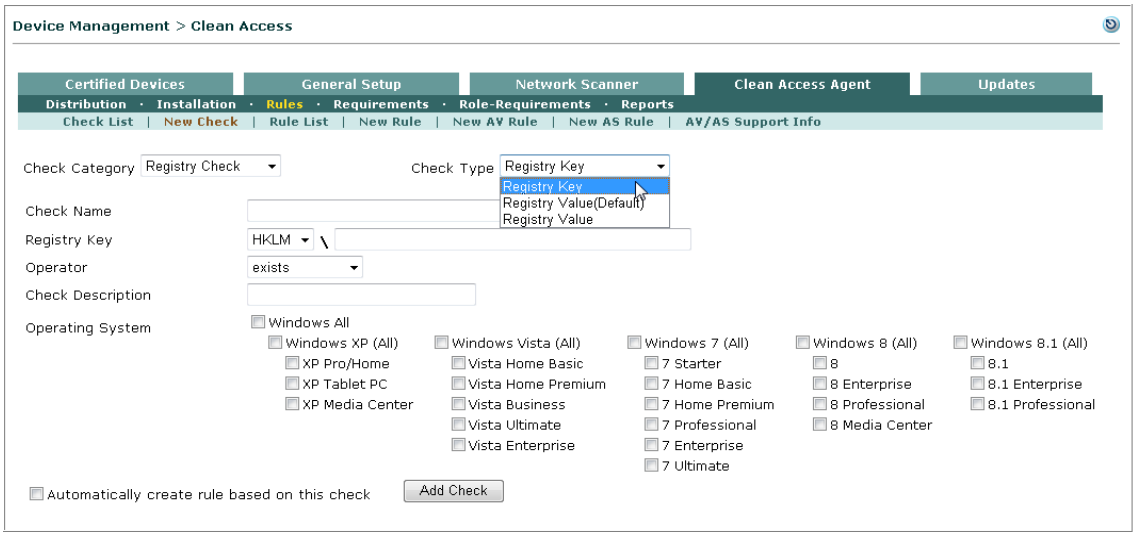
Step 7 If desired, select "**Automatically create rule based on this check**". In this case, the rule is automatically populated with the check when added and is named "*checkname-rule*".

Step 8 Click **Add Check** when finished.

Registry Checks

- **Registry Key**—Checks whether a specific key exists in the registry.
- **Registry Value (Default)**—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
- **Registry Value**—Checks whether a named registry key exists or has a particular value, version, or modification date.

Figure 9-32 Registry Check Types



a. For the **Registry Key** field, select the area of the client registry:

- **HKLM** – HKEY_LOCAL_MACHINE
- **HKCC** – HKEY_CURRENT_CONFIG
- **HKCU** – HKEY_CURRENT_USER
- **HKU** – HKEY_USERS
- **HKCR** – HKEY_CLASSES_ROOT

Then type the path to be checked.

For example: `HKLM \SOFTWARE\Symantec\Norton AntiVirus\version`

b. For a Registry Value search, enter a **Value Name**.

c. For Registry Value searches, enter a **Value Data Type**:

1. For a **"Number" Value Data Type** (**Note:** REG_DWORD is equivalent to Number), choose one of the following **Operators** from the dropdown: equals, greater than, less than, does not equal, greater than or equal to, less than or equal to
2. For a **"String" Value Data Type** choose one of the following **Operators** from the dropdown: equals, equals (ignore case), does not equal, starts with, does not start with, ends with, does not end with, contains, does not contain.
3. For a **"Version" Value Data Type** choose one of the following **Operators** from the dropdown: earlier than, later than, same as.
4. For a **"Date" Value Data Type**, choose one of the following **Operators** from the dropdown: earlier than, later than, same as.

d. If specifying a **"Date" Value Data Type**, also choose one of two values to check. This allows you to specify "older than" or "newer than" by more than/fewer than x days to the current date.

- Type the date/time of the client machine in **mm/dd/yyyy hh:MM:ss** format.
- Choose the **CAM date**, **+** or **-** from the dropdown, and type the number of days.

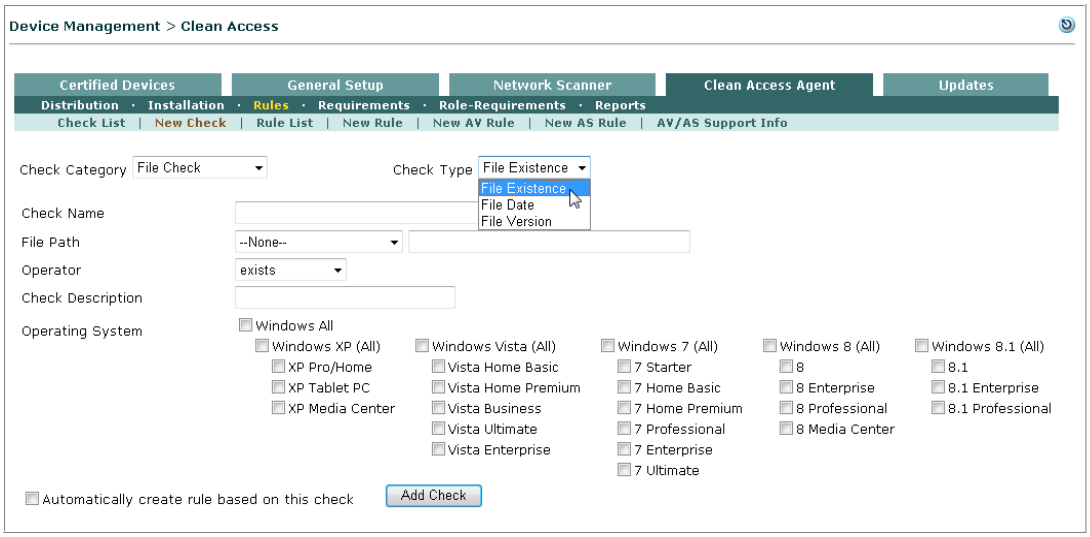
e. Type the **Value Data** for a Registry Value search.

Note For the "String" Value Data Type, the maximum length for a string is 256 characters.

File Checks

- **File Existence**—Checks whether a file exists on the system.
- **File Date**—Checks whether a file with a particular modification or creation date exists on the system.
- **File Version**—Checks whether a particular version of a file exists on the system.

Figure 9-33 File Check Types



a. For **File Path**, select:
   - **SYSTEM_DRIVE** – checks the C:\ drive
   - **SYSTEM_ROOT** – checks the root path for Windows systems
   - **SYSTEM_32** – checks C:\WINDOWS\SYSTEM32
   - **SYSTEM_PROGRAMS** – checks C:\Program Files

b. For **Operator**, select:
   - **exists** or **does not exist** – File Existence check
   - **earlier than**, **later than**, **same as** – File Date or File Version check

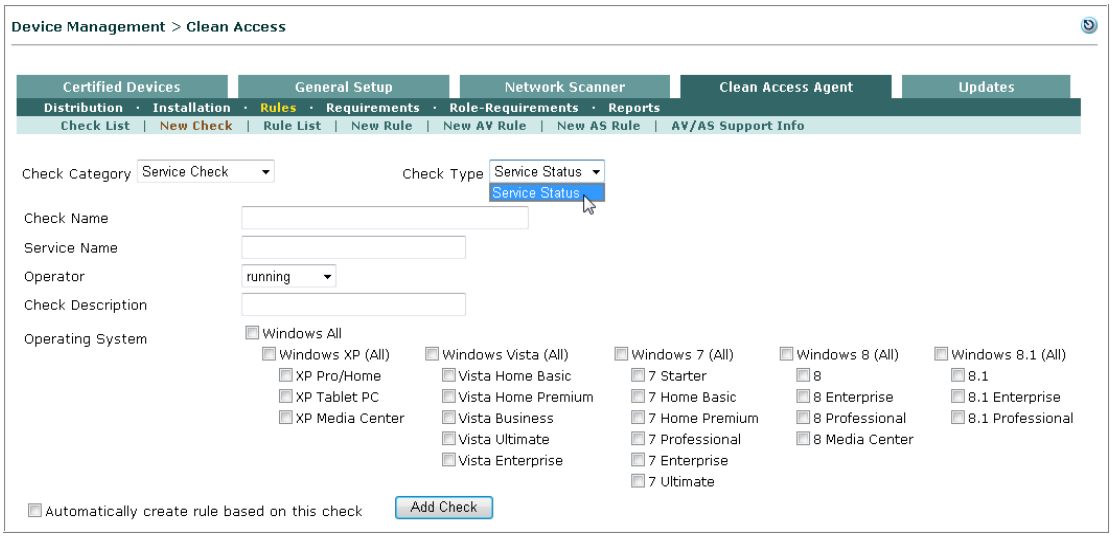
c. For a **File Date** check type, also choose one of two values to check for **File Date**. This allows you to specify "older than" or "newer than" by more than/fewer than x days to the current date.
   - Type the date/time of the client machine in **mm/dd/yyyy hh:MM:ss** format
   - Choose the **CAM date**, **+** or **-** from the dropdown, and type the number of days

d. For a **File Date** check type, select a **File Date Type**:
   - **Creation date**
   - **Modification date**

Service Check

- **Service Status** – Whether a service is currently running on the system.

Figure 9-34 Service Check Type



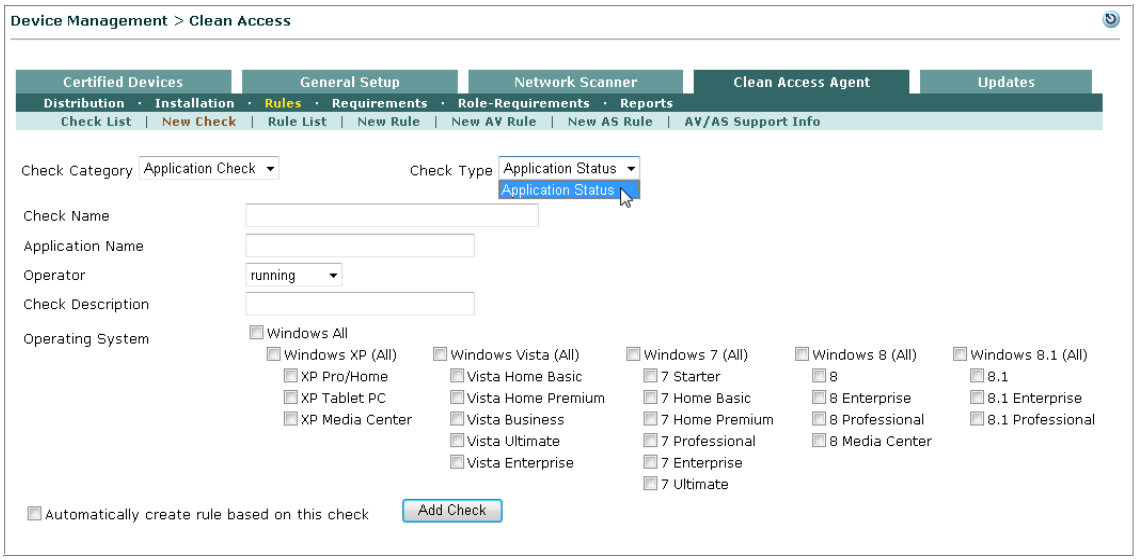
a. Enter a **Service Name**. The **Service Name** in this context is the name that comes up when a user double-clicks on the service in Microsoft Management Console with a "Service Name:" prefix. For example, "Windows Firewall/Internet Connection Sharing (ICS)" would need to be configured as "SharedAccess" in the **Service Name** field to check for the service.

b. Select an **Operator**:
   - **running**
   - **not running**

Application Check

- **Application Status** – Whether an application is currently running on the system.

Figure 9-35 Application Check Type



a. Enter an **Application Name**.

b. Select an **Operator**: **running** or **not running**.

Create a Custom Rule

A rule is an expression made up of checks and operators. A rule is the unit used by the Agent to assess a posture on a particular operating system. The result of the rule expression is considered to assess compliance with the Agent requirement. A rule can be made up of a single check or it can have multiple checks combined with Boolean operators. Table 9-15 shows the operators along with their order of evaluation.

Table 9-15 Rule Operators

Priority	Operator	Description
1	()	parens for evaluation priority
2	!	not
3	&	and
3	|	or

Operators of equal priority are evaluated from left to right. For example, a rule may be defined as follows:

```
adawareLogRecent & (NorAVProcessIsActive | SymAVProcessIsActive)
```

The `adawareLogRecent` check and either the `NorAVProcessIsActive` check or the `SymAVProcessIsActive` check must be satisfied for the rule to be considered met. Without parentheses, the following would be implied:

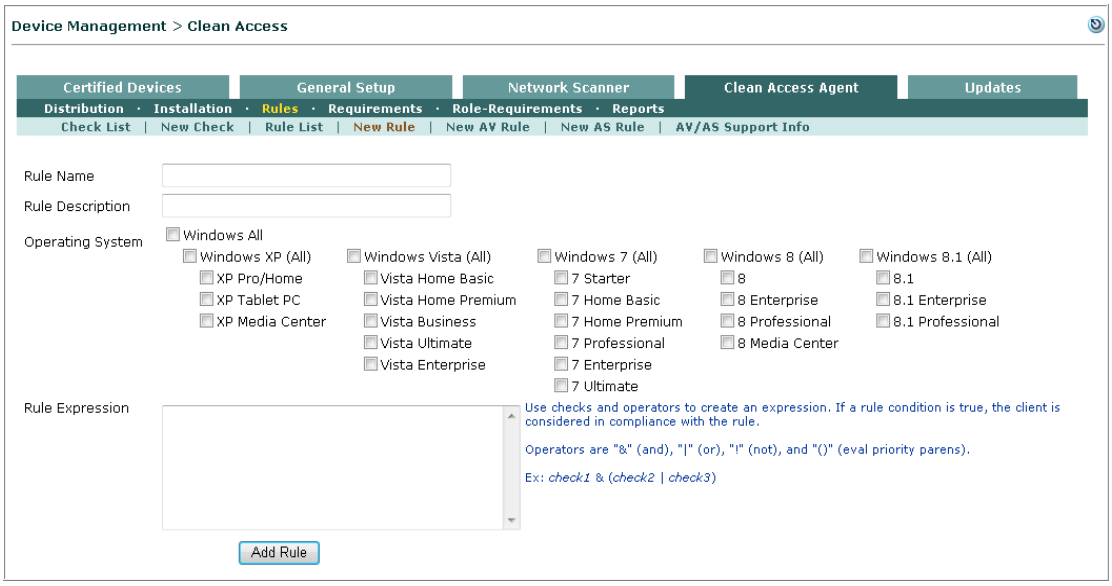
```
(adawareLogRecent & NorAVProcessIsActive) | SymAVProcessIsActive
```

In this case, either `SymAVProcessIsActive` or both of the first two checks must be true for the rule to be considered met.

Use the following steps to create a custom Rule.

Step 1 In the **Clean Access Agent** tab, click the **Rules** submenu link and then **New Rule**.

Figure 9-36 New Rule



Step 2 Type a unique **Rule Name**.

Step 3 Enter a **Rule Description**.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 4 Select the **Operating System** for which the rule applies. If Updates have been downloaded, the pre-configured checks for that operating system appear in the **Checks for Selected Operating System** list below.

Step 5 Create the **Rule Expression** by combining checks and operators. Use the list to select the names of checks and copy and paste them to the **Rule Expression** text field. Use the following operators with the checks: () (evaluation priority), **!** (not), **&** (and), | (or).

For example:

```
adawareLogRecent & (NorAVProcessIsActive | SymAVProcessIsActive)
```

For a simple rule that tests a single check, simply type the name of the check:

```
SymAVProcessIsActive
```

Step 6 Click **Add Rule**.

The console validates the rule and, if formed correctly, the rule appears in the **Rule List**. From there, you can delete the rule, modify it, or copy it (create a new rule by copying this one).

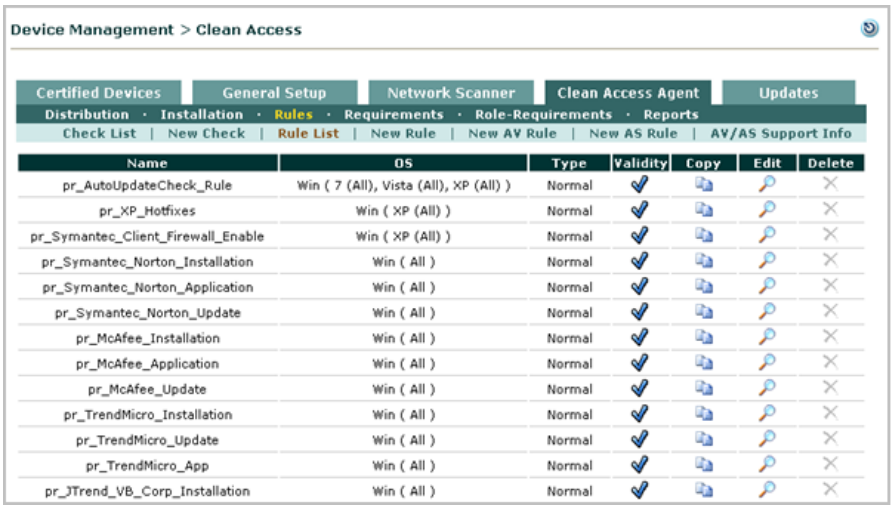
Validate Rules

The Clean Access Manager automatically validates rules and requirements as they are created. Invalid rules have incompatibilities between checks and rules, particularly those relating to the target operating system. These errors can arise when you create checks and rules for a particular operating system but later change the operating system property for a check. In this case, a rule that uses the check and which is still applicable for the formerly configured operating system is no longer valid. Rule validation detects these and other errors.

The **Validity** column under **Device Management > Clean Access > Clean Access Agent > Rules > Rule List** displays a blue checkmark if the rule is valid and a red "X" if the rule is invalid. Highlight this icon with your mouse to reveal which check is causing the rule to be invalid, in the form:

```
Invalid rule [rulename], Invalid check [checkname] in rule expression.
```

Figure 9-37 Rule List



Use the following steps to correct an invalid Rule.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Rules > Rule List**.

Step 2 Click the **Edit** icon for the invalid rule.

Step 3 Correct the invalid **Rule Expression**. If the rule is invalid because a check has been deleted, make sure you associate the rule with a valid check.

Step 4 Make sure the correct **Operating System**. is selected.

Step 5 Make sure the **Requirement met if:** expression is correctly configured.

Step 6 Click **Save Rule**.

Step 7 Make sure any requirement based on this rule is also corrected as described in Validate Requirements, page 9-93.

Create a Custom Requirement

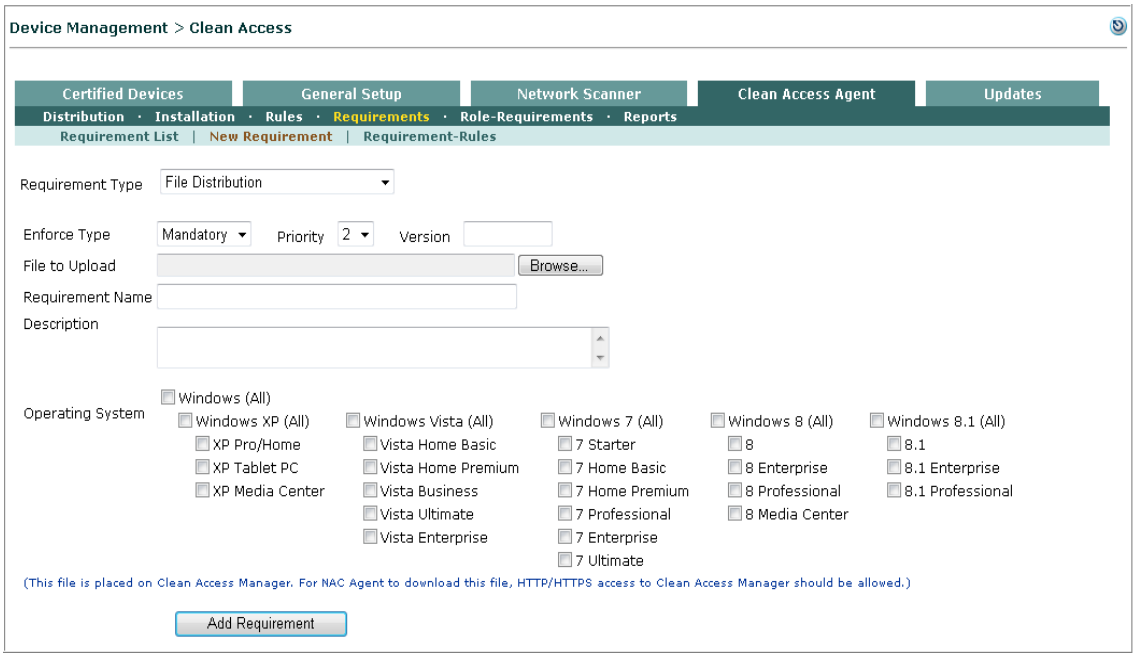
Custom requirements map a specified collection of rules for an operating system to the files, distribution links, or instructions that you want pushed to the user via Agent dialogs. Custom requirements can point to installation files or links where software can be downloaded. For local checks not associated with a specific installation file, the requirement can map the rule to an informational message, for example, instructing the user to remove software or run a virus check. A new requirement can be created at any time in the configuration process. However, the requirement must be associated to both a rule for an operating system and a user role before it can take effect.

Create File Distribution/Link Distribution/Local Check Requirement

Use the following steps to configure a custom requirement.

Step 1 In the **Clean Access Agent** tab, click the **Requirements** submenu link and then **New Requirement**.

Figure 9-38 New Requirement (File Distribution)



Step 2 Select a **Requirement Type**:

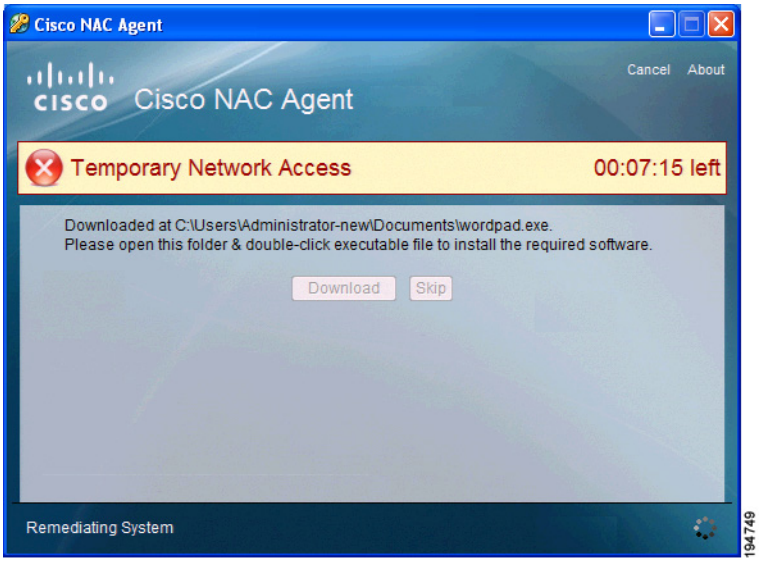
- **File Distribution** – This distributes the required software directly by making the installation package available for user download using the Agent. In this case, the file to be downloaded by the user is placed on the CAM using the **File to Upload** field. (The maximum file size you can make

available to users via File Distribution is 50MB.) For the Agent to download this file, you should create a traffic policy allowing HTTPS access only to the CAM for the Temporary role. See Adding Traffic Policies for Default Roles, page 8-27.

You can also use the File Distribution requirement type to search the client machine for a specific file that is different from the one you want users to download. That way, you can force users who do not yet have the correct file to get it via the File Distribution requirement and allow users who already have the file installed to simply pass this particular step in the posture assessment process.

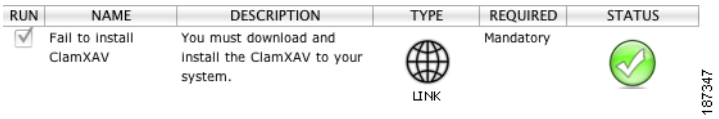
Note For NAC Appliance Release 4.8 and later, the File Distribution requirement type works only when the Agent version is 4.8.0.32 or later. If you are using CAM/CAS version 4.8 or later with an Agent version earlier than 4.8.0.32, then either use the Link Distribution requirement or upgrade the Agent to the latest version to use the File Distribution.

Figure 9-39 Example Cisco NAC Agent File Distribution Dialog



- **Link Distribution** – This refers users to another web page where the software is available, such as a software download page. Make sure the Temporary role is configured to allow HTTP (and/or HTTPS) access to the link.

Figure 9-40 Example Mac OS X Agent Assessment Report Link Distribution Requirement Display



- **Local Check** – This is used when creating checks not associated with installable software, for example, to check if Windows Update Service (Automatic Updates) is enabled, or to look for software that should not be on the system. (The Mac OS X Agent Assessment Report window displays Local Check requirements using a “Message” icon.)

Figure 9-41 Example Mac OS X Agent Assessment Report Local Check Requirement Display



Step 3 Choose an **Enforce Type** from the dropdown menu:

- **Mandatory**—Enforce requirement.The user is informed of this requirement and cannot proceed or have network access unless the client system meets it.
- **Optional**— Do not enforce requirement. The user is informed of the requirement but can bypass it if desired (by clicking **Next/Skip** in the Agent dialog). The client system does not have to meet the requirement for the user to proceed or have network access.
- **Audit**—Silently audit. The client system is checked "silently" for the requirement without notifying the user, and a report is automatically generated and sent back to the CAS. (Audit requirements do not appear in the user's Assessment Report window.) The report results (pass or fail) do not affect user network access.

Refer to Configuring an Optional/Audit Requirement, page 9-94 for more details.

Step 4 Specify the **Priority** of the requirement. Requirements with the lowest number (e.g "1") have the highest priority and are performed first. If a requirement fails, the remediation instructions configured for the requirement are pushed to the user without additional requirements being tested. Therefore you can minimize processing time by putting the requirements that are most likely to fail at a higher priority.

Step 5 You can enable and configure Auto Remediation using the Agent for a **Link Distribution** requirement type only. Refer to Configuring Auto Remediation for Requirements, page 9-98 for details.

Note The Cisco NAC Web Agent does not support Auto Remediation.

Step 6 The **Version** field lets you keep track of various versions of a requirement. This is particularly useful when there are updates to the required software. You can use any versioning scheme you like, such as numbers (1, 2, 3), point numbers (1.0), or letters.

Step 7 If you chose **File Distribution** as the Requirement Type, click **Browse** next to the **File to Upload** field and navigate to the folder where you have the installation file (.exe) for the required software.

Step 8 If you chose **Link Distribution** as the Requirement Type, enter the URL of the web page where users can get the install file or patch update in the **File Link URL** field.

Note The Mac OS X Agent does not support automatic remediation. Therefore, the Remediation functions that appear on the New Requirement configuration page (Remediation **Type**, **Interval**, and **Retry Count**) when you choose the **AV Definition Update** or **AS Definition Update** requirement types do not serve any purpose when creating requirements for Macintosh client remediation.

Step 9 For the **Requirement Name** type a unique name to identify the system requirement. The name will be visible to users on the Agent dialogs.

Step 10 In the **Description** field, type a description of the requirement and instructions for the benefit of your users. Note the following:

- **File Distribution** displays a **Download** button on the Agent.
- **Link Distribution** displays a **Go To Link** button on the Agent.
- **Local Check** displays a **Re-Scan** button on the Agent.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 11 Select the **Operating System** for which the requirement applies (you must choose at least one).

Step 12 Click **Add Requirement** to save the settings for the download requirement.

Step 13 The requirement appears in the **Requirement List**.

Figure 9-42 shows an example of how requirement configuration fields display in the Mac OS X Agent.

Figure 9-42 Mac OS X Agent Requirements (User Display Example)

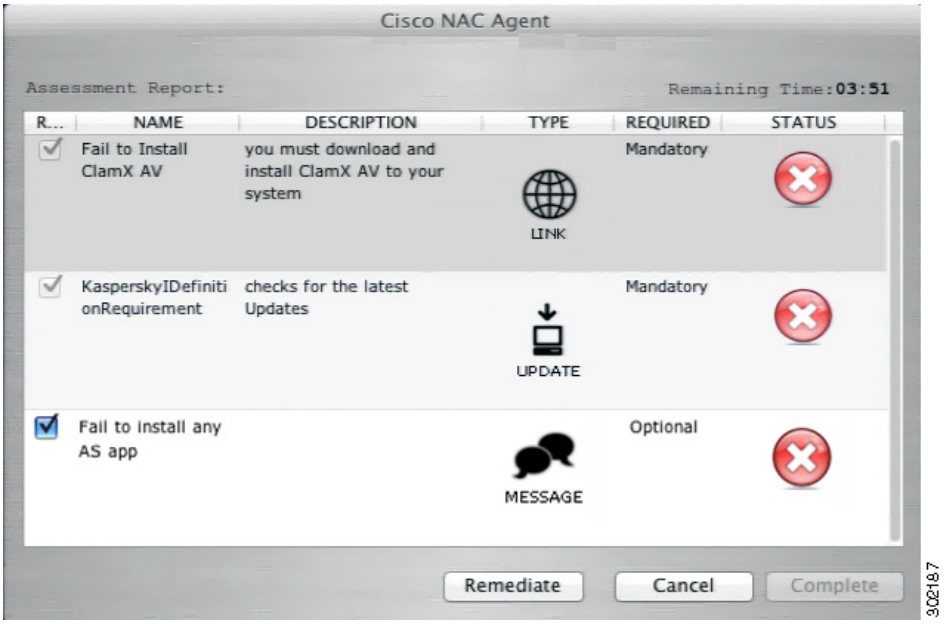
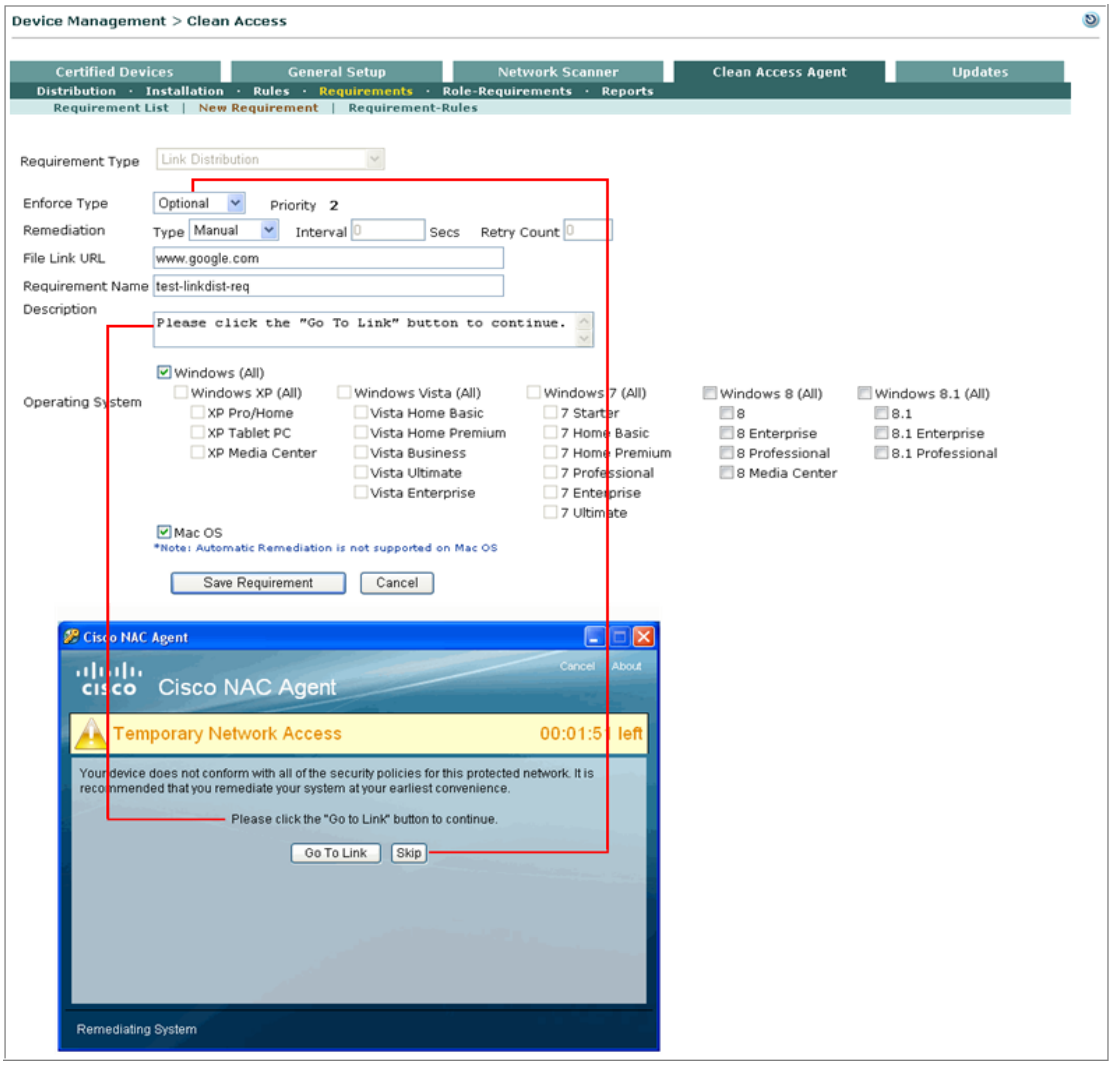


Figure 9-43 shows an example of how requirement configuration fields display in the Cisco NAC Agent.

Figure 9-43 Example Optional Link Distribution Requirement—Cisco NAC Agent on Windows XP



Configuring a Launch Programs Requirement

Note The Cisco NAC Agent is required to use this feature. This feature applies to Windows 8.1/8/7/Vista/XP machines only. The Mac OS X Agent and the Cisco NAC Web Agent do not support this requirement type.

The Launch Programs Requirement Type allows administrators to launch a qualified (signed) remediation program through the Agent. The administrator can create a check/rule condition; upon its failure, the administrator can configure to launch any remediation program to fix the machine. Multiple programs are permitted, and they are launched in the same sequence as specified by the administrator.

The Agent launches the programs in two ways, depending on whether the user has or does not have admin user privileges on the device.

When Cisco NAC is configured to launch an application as a remediation, the application gets launched and is available in the task manager, but the UI is not visible to the user, irrespective of whether the user is logged in as admin or not. Since Launch program remediation feature is modified from user privilege to system privilege, NAC Agent allows UAC Elevation for all Launch program remediation actions. See also the caveat CSCui73412 in *Release Notes for Cisco NAC Appliance, Version 4.9(4)*.

Launch Programs With Admin Privileges

If the user has admin privileges on the client machine, any program that is an executable is qualified. The program is launched directly and digital signing and verification of the application are not required.

Launch Programs Without Admin Privileges

The executable must have:

- A valid digital signature signed by certificates with specific field value(s)
- File version information with specific item value(s)

Note also that:

- The executable must be signed with a code signing certificate with a proper chain of certificates. The code signing certificate must be installed on the client machine.
- The root certificate must also be installed on the client machine and must be in the Trusted Root Certification Authority on Windows.
- **You must create a registry key that is particular to the executable being run in addition to installing the certificate.** Refer to How the Agent Verifies Digital Signature and Trust on an Executable Program, page 9-86 for details.

Note For non-admin users, if you want to configure Auto Remediation and launch a program (for example, a Microsoft KB patch), the signature check may fail if the executable is available on a network share, even if it is a mapped drive. It is recommended to copy the files to your local system and execute them. Starting from Release 4.9(1), non-admin users can set the SignatureCheck parameter to “1” in the Configuration file to check the signature. See also Cisco NAC Agent Verifying Launch Program Executable for Trusted Digital Signature.

How the Agent Verifies Digital Signature and Trust on an Executable Program

On client machines where users will launch executables, you must add a Trust<*N*> key in the Windows registry for the executable you want to run. It is the administrator's responsibility to populate the required registry keys for the programs to be trusted by the Cisco NAC Agent service. The Cisco NAC Agent verifies the launch program for a trusted digital signature as follows:

1. Verifies the digital signature - Ensures the digital signature is trusted.
2. Verifies the signer certificate information based on the information in the registry.

The related registry structure appears as follows:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CCAAgentStub\Trust<N>\
Certificate\2.5.4.3
\FileVersionInfo\ProductName
```

Where:

- <*N*> is a numeric number.
- For the entries under **Certificate**, each value can be exact case-insensitive.
- For the entries under **FileVersionInfo**, each value must appear in the corresponding value in the file information stream, and can also be case-insensitive.
- All the entries under **Certificate** and **FileVersionInfo** must be satisfied (AND operations) to qualify as a trusted target.
- If any of the **Trust**<*N*> chain is satisfied, the target is qualified to launch.

For example, the following key-value pairs in the registry qualify Cisco NAC Agent to be launched as an application by non-admin:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CCAAgentStub\Trust0\Certificate\ 2.5.4.3 with a value of "Cisco Systems"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CCAAgentStub\Trust0\ FileVersionInfo\ProductName with a value of "Cisco NAC Agent"

Administrators should add registry entries to qualify all applications users will launch on client machines. See Table 9-16 for a list of supported keys,

Table 9-16 Supported Launch Program Executable Keys for Trusted Digital Signature

Registry Key	Default Value (Decimal)	Valid Range	Supported Value Names
Location: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CCAAgentStub			
Trust<*N*>	—	0 and above	The Trust<*N*> chain is a digital signature for the executable that the Clean Access Agent Stub uses to determine whether or not Windows can trust the executable before launching.

Table 9-16 Supported Launch Program Executable Keys for Trusted Digital Signature (continued)

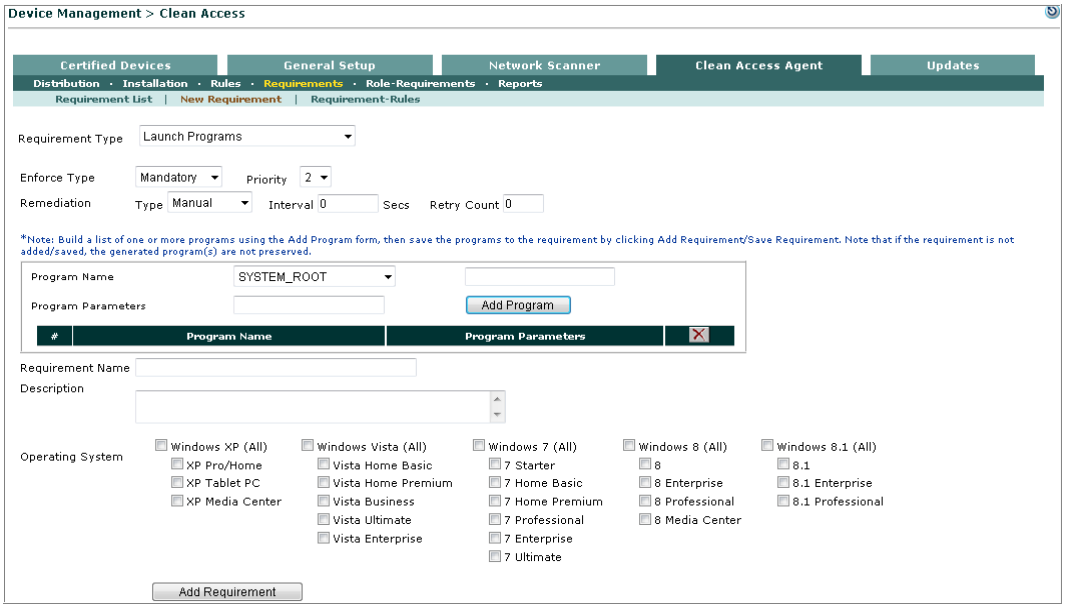
Registry Key	Default Value (Decimal)	Valid Range	Supported Value Names
Certificate	—	—	• 2.5.4.3 - COMMON_NAME or • 2.5.4.3 - SUBJECT_NAME • 2.5.4.4 - SUR_NAME • 2.5.4.5 - DEVICE_SERIAL_NUMBER • 2.5.4.6 - COUNTRY_NAME • 2.5.4.7 - LOCALITY_NAME • 2.5.4.8 - STATE_OR_PROVINCE_NAME • 2.5.4.9 - STREET_ADDRESS • 2.5.4.10 - ORGANIZATION_NAME • 2.5.4.11 - ORGANIZATIONAL_UNIT_NAME • 2.5.4.12 - TITLE • 2.5.4.13 - DESCRIPTION • 2.5.4.14 - SEARCH_GUIDE • 2.5.4.15 - BUSINESS_CATEGORY • 2.5.4.16 - POSTAL_ADDRESS • 2.5.4.17 - POSTAL_CODE • 2.5.4.18 - POST_OFFICE_BOX • 2.5.4.19 - PHYSICAL_DELIVERY_OFFICE_NAME • 2.5.4.20 - TELEPHONE_NUMBER
FileVersionInfo	—	—	• ProductName • CompanyName • FileDescription • FileVersion • InternalName • LegalCopyright • OriginalFileName • ProductVersion • Comments • LegalTrademarks • PrivateBuild • SpecialBuild

Create a Launch Programs Requirement

Use the following steps to configure a Launch Programs requirement.

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**.

Figure 9-44 New Launch Program Requirement



Step 2 For **Requirement Type** choose **Launch Programs**.

Step 3 Choose an **Enforce Type** from the dropdown menu:

- **Mandatory**—Enforce requirement.The user is informed of this requirement and cannot proceed or have network access unless the client system meets it.
- **Optional**— Do not enforce requirement. The user is informed of the requirement but can bypass it if desired (by clicking **Next/Skip** in the Agent dialog). The client system does not have to meet the requirement for the user to proceed or have network access.
- **Audit**—Silently audit. The client system is checked "silently" for the requirement without notifying the user, and a report is generated. The report results (pass or fail) do not affect user network access.

  Refer to Configuring an Optional/Audit Requirement, page 9-94 for details.

Step 4 Choose the **Priority** of execution for this requirement on the client. A high priority (e.g. 1) means this requirement is checked on the system ahead of all other requirements (and appears in the Agent dialogs in that order). Note that if a Mandatory requirement fails, the Agent does not continue past that point until that requirement succeeds.

Step 5 If you want to enable and configure Auto Remediation for the Agent:

a. Choose the **Remediation Type [Manual | Automatic]** from the dropdown menu. Choosing **Manual** preserves previous Agent behavior. The user has to click through each of the requirements using the **Next/Skip** button in the Agent. Choosing **Automatic** sets the Agent to perform Auto Remediation, where the Agent automatically performs updates or launches required programs on the client after the user logs in.

b. If you configure the requirement to use automatic remediation, specify the **Interval** in seconds (the default interval is 0). Depending on the requirement type, this interval either sets the delay before the Agent re-attempts remediation or sets the total time allowed for a particular remediation process.

c. Enter the **Retry Count []**. Specifying a retry count sets a limit on the number of times the Agent automatically retries the requirement if it initially fails. (The default retry count setting is 0.)

For details on configuring Auto Remediation, see Configuring Auto Remediation for Requirements, page 9-98.

Note The Cisco NAC Web Agent does not support Auto Remediation.

Step 6 Configure the program to be launched as follows:

a. For the **Program Name**, choose the root location from which to launch the program from the dropdown: **SYSTEM_DRIVE**, **SYSTEM_ROOT**, **SYSTEM_32**, **SYSTEM_PROGRAMS**, or **None**, and type the name of the program executable in the adjoining text field.

b. If a more specific path or program parameters are needed, type them in the **Program Parameters** text field.

c. Click **Add Program**. This adds the **Program Name** and **Program Parameters** to the sublist of programs to launch for the requirement.

d. Configure more programs to add, or click the **Delete** checkbox to remove programs from the list.

Step 7 When done configuring the program or list of programs to added, type the **Requirement Name**.

Step 8 Type a **Description** to be displayed to users.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 9 Click the checkbox for the Windows **Operating System** for which this requirement applies.

Step 10 Click **Add Requirement**.

Map Requirements to Rules

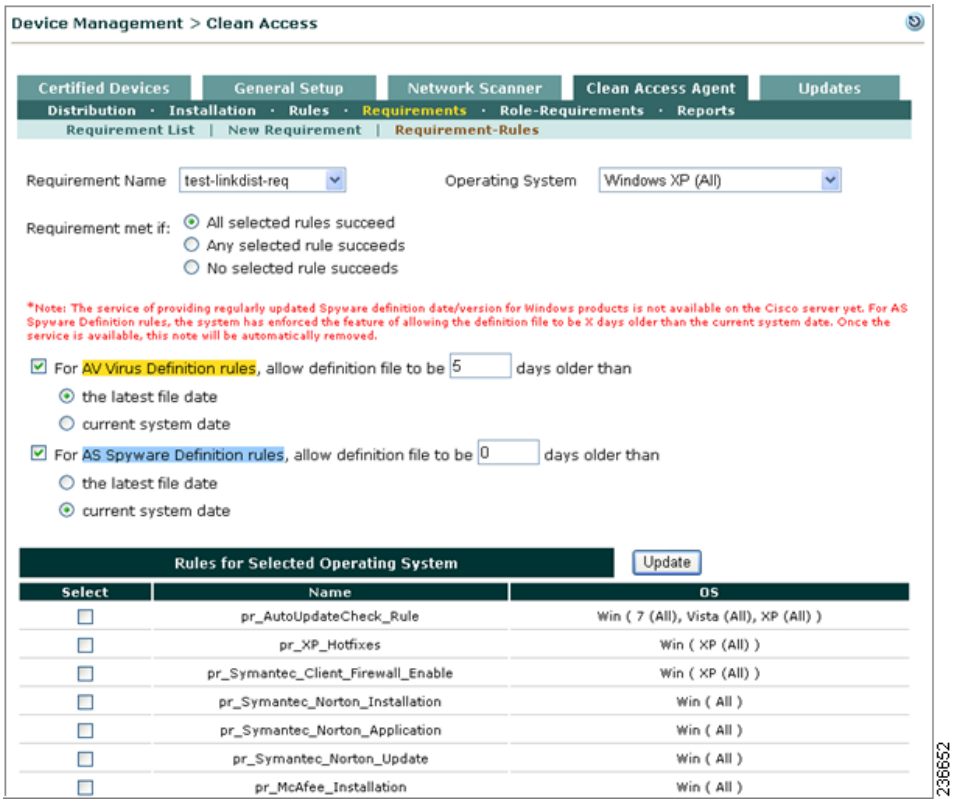
Once the requirement is created and the remediation links and instructions are specified, map the requirement to a rule or set of rules. A requirement-to-rule mapping associates the ruleset that checks whether the client system meets the requirement to the user requirement action (Agent button, instructions, links) needed for the client system to comply.

Note The Mac OS X Agent does not support custom checks and custom rules. You can only assign AV and AS rules to the Link Distribution, Local Check, AV Definition Update, and AS Definition Update requirement types for Mac OS X posture remediation.

Use the following steps to map a requirement to rules.

Step 1 In the **Clean Access Agent** tab, click the **Requirements** submenu and then open the **Requirement-Rules** form.

Figure 9-45 Requirement-Rules Mapping


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Distribution · Installation · Rules · Requirements · Role-Requirements · Reports
Requirement List | New Requirement | Requirement-Rules
Requirement Name
test-linkdist-req
Operating System
Windows XP (All)
Requirement met if:
All selected rules succeed
Any selected rule succeeds
No selected rule succeeds
*Note: The service of providing regularly updated Spyware definition date/version for Windows products is not available on the Cisco server yet. For AS Spyware Definition rules, the system has enforced the feature of allowing the definition file to be X days older than the current system date. Once the service is available, this note will be automatically removed.
For AV Virus Definition rules, allow definition file to be 5 days older than
the latest file date
current system date
For AS Spyware Definition rules, allow definition file to be 0 days older than
the latest file date
current system date
Rules for Selected Operating System
Update
Select
Name
OS
pr_AutoUpdateCheck_Rule
Win (7 (All), Vista (All), XP (All))
pr_XP_Hotfixes
Win (XP (All))
pr_Symantec_Client_Firewall_Enable
Win (XP (All))
pr_Symantec_Norton_Installation
Win (All)
pr_Symantec_Norton_Application
Win (All)
pr_Symantec_Norton_Update
Win (All)
pr_McAfee_Installation
Win (All)
236852

Step 2 From the **Requirement Name** menu, select the requirement to map.

Step 3 Verify the operating system for the requirement in the **Operating System** menu. The **Rules for Selected Operating System** list will be populated with all rules available for the chosen OS.

Step 4 For the **Requirements met if** option, choose one of the following options:

- **All selected rules succeed**—if all the rules must be satisfied for the client to be considered in compliance with the requirement.
- **Any selected rule succeeds**—if at least one selected rule must be satisfied for the client to be considered in compliance with the requirement.
- **No selected rule succeeds**—if the selected rules must all fail for the client to be considered in compliance with the requirement.

If clients are not in compliance with the requirement, they will need to install the software associated with the requirement or take the steps instructed.

Step 5 For AV Virus Definition Rules (yellow background) and AS Spyware Definition rules (blue background), you can optionally configure the CAM to allow definition files on the client to be a number of days older than what the CAM has available from **Updates** (see **Rules > AV-AS Support Info** for the latest product file dates). This allows you to configure leeway into a requirement so that if no new virus/spyware definition files are released from a product vendor, your clients can still pass the requirement.

Click the checkbox for either:

- **For AV Virus Definition rules, allow definition file to be x days older than:**
- **For AS Spyware Definition rules, allow definition file to be x days older than:**

Type a number in the text box. The default is "**2**" indicating the definition date cannot be older than the file/system date.

Choose either:

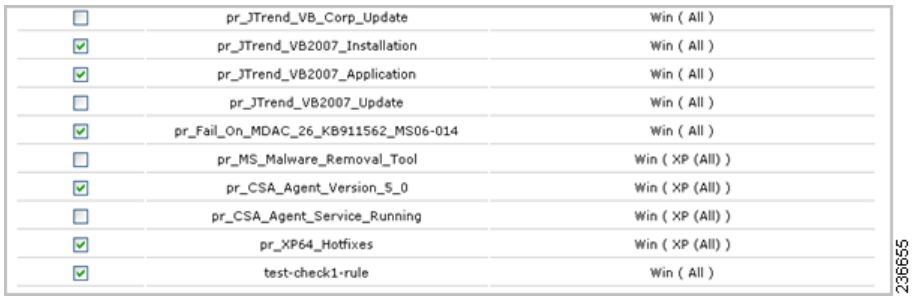
- **Latest file date**—This allows the client definition file to be older than the latest virus/spyware definition date on the CAM by the number of days you specify.
- **Current system date**—This allows the client definition file to be older than the CAM's system date when the last **Update** was performed by the number of days you specify.

Note For AS Spyware Definition rules, the system will enforce this feature (allowing the definition files to be X days older then the current system date) until Cisco Update service is available to regularly update the date/version for Spyware definition files.

When this feature is configured for a requirement, the Agent checks for the definition date of the AV/AS product then verifies whether the date meets the requirement. If the Agent cannot detect the definition date (i.e., def date detection is not supported for that product), the system ignores this feature and the Agent checks whether the client has the latest definition version.

Step 6 Scroll down the page and click the **Select** checkbox next to each rule you want to associate with the requirement. The rules will be applied in their order of priority, as described in Table 9-15 on page 9-77.

Figure 9-46 Select Rules to Map to Requirement


pr_JTrend_VB_Corp_Update Win (All)
pr_JTrend_VB2007_Installation Win (All)
pr_JTrend_VB2007_Application Win (All)
pr_JTrend_VB2007_Update Win (All)
pr_Fail_On_MDAC_26_KB911562_MS06-014 Win (All)
pr_MS_Malware_Removal_Tool Win (XP (All))
pr_CSA_Agent_Version_5_0 Win (XP (All))
pr_CSA_Agent_Service_Running Win (XP (All))
pr_XP64_Hotfixes Win (XP (All))
test-check1-rule Win (All)
236655

Step 7 Click **Update**.

Apply Requirements to User Roles

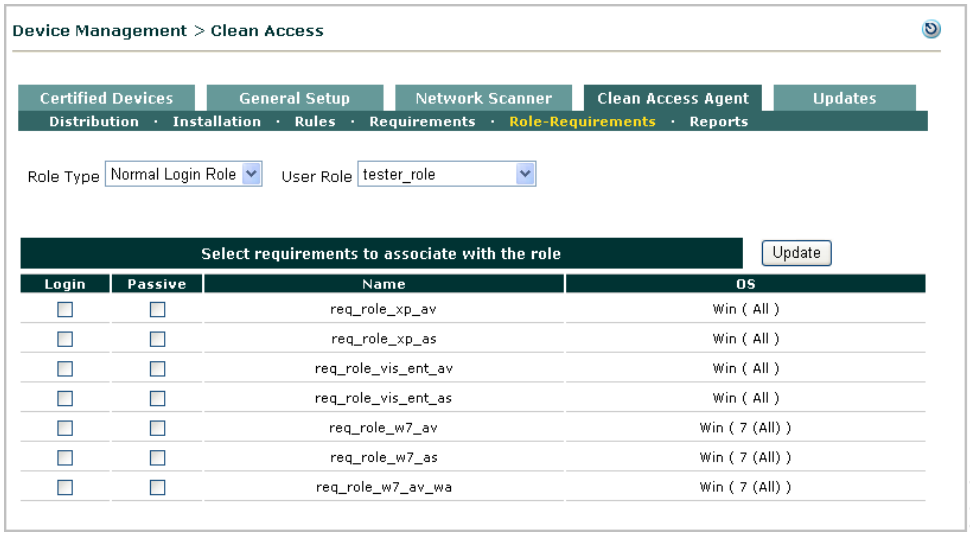
Once requirements are created, configured with remediation steps, and associated with rules, they need to be mapped to user roles. This last step applies your requirements to the user groups in the system.

Note Make sure you already have normal login user roles created as described in Create User Roles, page 6-2.

Use the following steps to map requirements to a user role.

Step 1 In the **Clean Access Agent** tab, click the **Role-Requirements** submenu link.

Figure 9-47 Role- Requirements Mapping



Step 2 From the **Role Type** menu, select the type of the role you are configuring. In most cases, this will be **Normal Login Role**.

Step 3 Select the name of the role from the **User Role** menu.

Step 4 Check the **Login** checkbox for each requirement you want to apply to users in the role during login.

Step 5 Check the **Passive** checkbox for each requirement you want to apply Passive Re-assessment. See Role Properties, page 6-9 for more details on Passive Re-assessment.

Step 6 Click **Update**.

Step 7 Before finishing, make sure users in the role are required to use the Agent. See Require Agent Login for Client Machines, page 9-3.

Validate Requirements

The Clean Access Manager automatically validates requirements and rules as they are created. The **Validity** column under **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement List** displays a blue checkmark if the requirement is valid and a red "X" if the requirement is invalid.

Highlighting red "X" icons (if any) with your mouse reveals which rule and which check is causing the requirement to be invalid, in the form:

```
Invalid rule [rulename] in package [requirementname] (Rule verification error: Invalid
check [checkname] in rule expression)
```

The requirement must be corrected and made valid before it can be used. Typically requirements/rules become invalid when there is an operating system mismatch.

To Correct an Invalid Requirement:

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**.

Step 2 Correct any invalid rules or checks as described in Validate Rules, page 9-79.

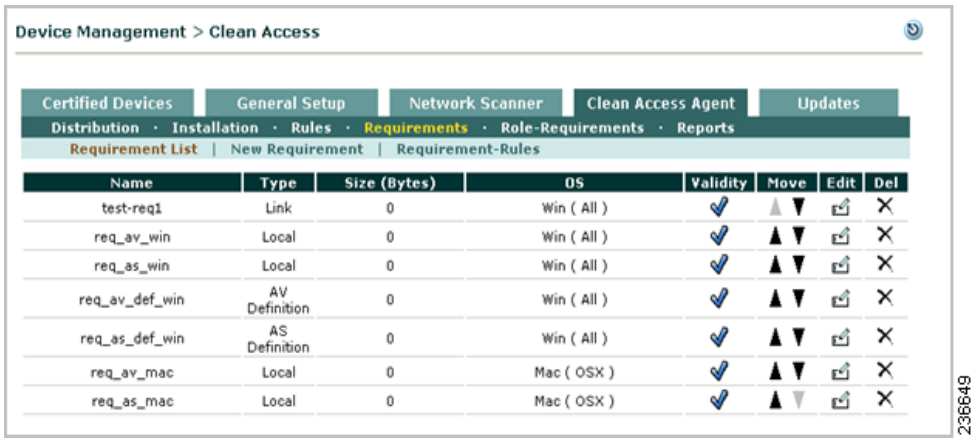
Step 3 Select the invalid **Requirement Name** from the dropdown menu.

Step 4 Select the **Operating System**.

Step 5 Make sure the **Requirement met if:** expression is correctly configured.

Step 6 Make sure the rules selected for the requirement are valid (blue checkmark in Validity column).

Figure 9-48 Requirement List



Configuring an Optional/Audit Requirement

You can make any requirement **Mandatory**, **Optional**, or **Audit**-only using the **Enforce Type** dropdown menu in the **New Requirement** or **Edit Requirement** form. Optional requirements allow you to view administrative reports for an Agent user without blocking the client from the network if the optional requirement fails. If an optional requirement fails, the user is put in the Temporary role and will see "Optional" preceding the name of the requirement in the Agent dialog; however the user can click **Next/Skip** and either proceed to the next requirement or to the network if no other requirements are configured.

If you want to provide an extended period of time for users to meet requirements without blocking them from the network, you can configure an optional requirement with instructions to comply by a certain date. You can later enforce the requirement at the specified date to make the requirement mandatory.

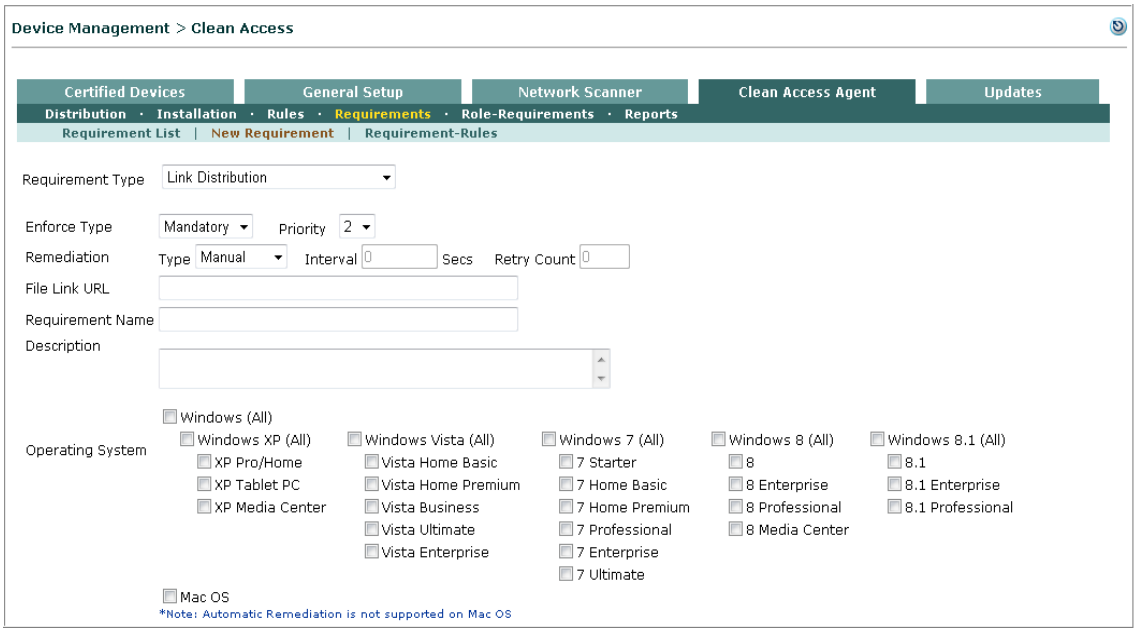
If you want to ensure that the client system is checked "silently" for the requirement without notifying the user, and that a report is generated and sent back to the CAS, you can configure an audit-only requirement which only reports results (pass or fail) and does not affect user network access.

Note If the Optional/Audit requirement fails while Passive Re-assessment (PRA) has been enabled, then the PRA report information will not be passed to the CAM. It is recommended to enable the Optional or Audit requirement along with Mandatory requirement so that the report information is passed to the CAM.

To create an Optional or Audit requirement:

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**.

Figure 9-49 Optional/Audit Requirement



Step 2 Choose a **Requirement Type** from the dropdown.

Step 3 Choose **Optional** (do not enforce) or **Audit** (silent assessment) as the **Enforce Type** from the dropdown menu.

For an **Optional** requirement, the user is informed of the requirement but can bypass it if desired (by clicking **Next/Skip** in the Agent dialog). The client system does not have to meet the requirement for the user to proceed or have network access. For an **Audit** requirement, the system generates audit reports, but no user dialogs appear on the client machine and the user's network access is unaffected.

Step 4 Choose the **Priority** of execution for this requirement on the client. A high priority (e.g. 1) means this requirement is checked on the system ahead of all other requirements (and appears in the Agent dialogs in that order). Note that if a Mandatory requirement fails, the Agent does not continue past that point until that requirement succeeds.

Note The Mac OS X Agent does not support automatic remediation. Therefore, the Remediation functions that appear on the New Requirement configuration page (Remediation **Type**, **Interval**, and **Retry Count**) do not serve any purpose when creating requirement types for Macintosh client remediation.

Step 5 If you want to enable and configure Auto Remediation for the Agent:

a. Choose the **Remediation Type [Manual | Automatic]** from the dropdown menu. Choosing **Manual** preserves previous Agent behavior. The user has to click through each of the requirements using the **Next/Skip** button in the Agent. Choosing **Automatic** sets the Agent to perform Auto Remediation, where the Agent automatically performs updates or launches required programs on the client after the user logs in.

b. If you configure the requirement to use automatic remediation, specify the **Interval** in seconds (the default interval is 0). Depending on the requirement type, this interval either sets the delay before the Agent re-attempts remediation or sets the total time allowed for a particular remediation process.

c. Enter the **Retry Count []**. Specifying a retry count sets a limit on the number of times the Agent automatically retries the requirement if it initially fails. (The default retry count setting is 0.)

For details on configuring Auto Remediation, see Configuring Auto Remediation for Requirements, page 9-98.

Note The Cisco NAC Web Agent does not support Auto Remediation.

Step 6 Configure specific fields for the requirement type.

Step 7 Type the **Requirement Name** for the optional requirement.

Step 8 Type instructions in the **Description** field to inform users that this is an optional requirement and that they can still proceed to the network by clicking the **Next/Skip** button on the Agent dialog. Note the following:

- **File Distribution** displays a **Download** button on the Agent.
- **Link Distribution** displays a **Go To Link** button on the Agent.
- **Local Check** displays a **Re-Scan** button on the Agent.
- **AV Definition Update** displays an **Update** button on the Agent.
- **AS Definition Update** displays an **Update** button on the Agent.
- **Windows Update** displays an **Update** button on the Agent.
- **Launch Programs** displays a **Launch** button on the Agent.
- **Windows Server Update Service** displays an **Update** button on the Agent.

Note Some of the default user messages in the Agent dialogs are very similar between various rules and/or requirements. To ensure the user clearly understands the remediation issue at hand, Cisco strongly recommends providing an appropriate message in this field describing the nature and purpose of the given function.

Step 9 Click the checkbox(es) for the **Operating System.**

Step 10 Click **Add Requirement**.

Optional requirements must be mapped to rules and user roles in the same way as mandatory requirements. Refer to Map Requirements to Rules, page 9-90 and Apply Requirements to User Roles, page 9-92 for details.

Figure 9-50 Example Cisco NAC Agent Dialog for Optional Requirement

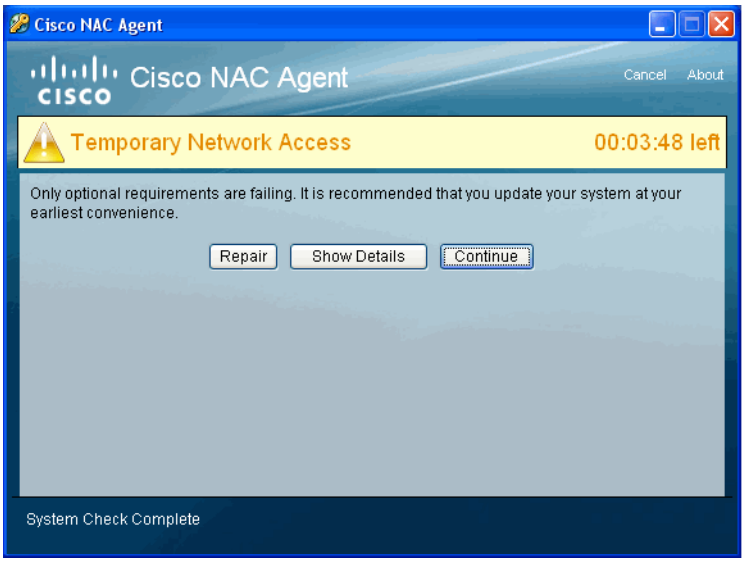
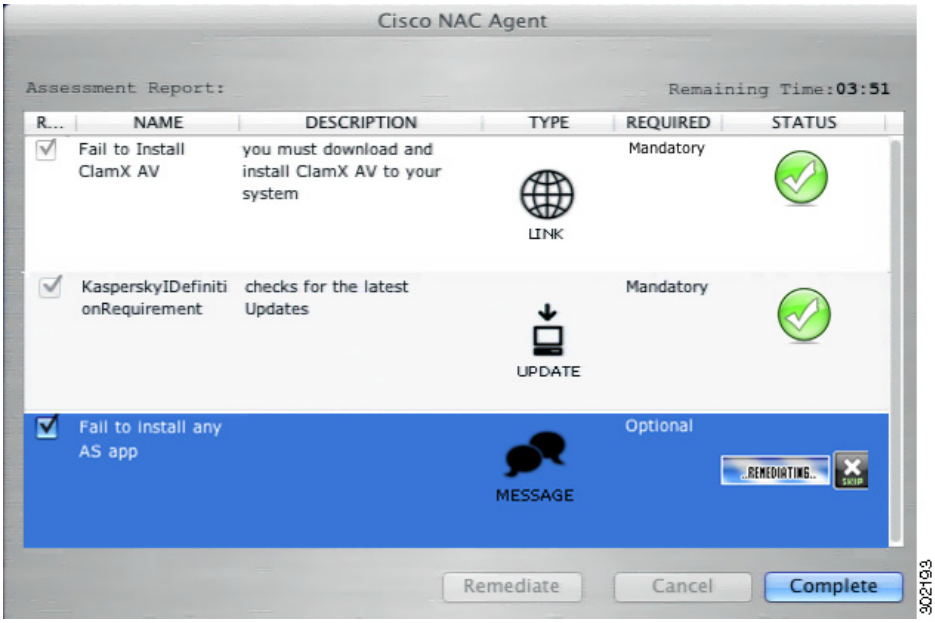


Figure 9-51 Example Mac OS X Agent Dialog for Optional Requirement



Configuring Auto Remediation for Requirements

You can configure Auto Remediation for all requirement types except File Distribution and Local Check.

Note This configuration example is specific to the Cisco Clean Access Agent. The Mac OS X Agent and Cisco NAC Web Agent do not support Auto Remediation.

To configure Auto Remediation:

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**, and select the **Requirement Type**. You can configure Auto Remediation for:

- Link Distribution
- AV Definition Update
- AS Definition Update
- Windows Update
- Launch Programs
- Windows Server Update Services

Step 2 Choose the **Enforce Type** [Mandatory | Optional | Audit] from the dropdown.

Step 3 Choose the **Remediation Type [Manual | Automatic]** from the dropdown.

Choosing **Manual** preserves the previous Agent behavior. The user has to click through each of the requirements using the **Next/Skip** button.

Choosing **Automatic** sets the Agent to perform Auto Remediation, where the Agent automatically performs updates or launches required programs on the client after the user logs in. The Agent automatically performs different actions depending on the requirement type, for example:

- Auto launches URL in the default browser for Link Distribution
- Auto updates AV/AS definition files on the client for AV/AS Definition Update
- Auto launches Windows Auto Update(s) (in background) for Windows Update
- Auto launches programs for Launch Programs
- Auto installs WSUS client updates for Windows Server Update Services

When you check the **Automatic** option, you can optionally configure how long the Agent waits before it retries the same requirement (**Interval**), and how many times the Agent retries the requirement if it initially fails on the client (**Retry Count**). The effect of these options is slightly different depending on the requirement type.

Note During **Auto Remediation** on the Agent, the resulting dialog displays only two buttons: **Details** and **Manual**. Clicking **Details** shows additional progress messages for the Auto Remediation. If Auto Remediation fails, the user can click the **Manual** button to change the Agent back to Manual mode, where the user has to click through each requirement.

Step 4 Enter a value for the **Interval [] Secs** setting:

- **Interval [] Secs**—Default is 0. Depending on the requirement type, this interval either sets the delay before the Agent re-attempts remediation or sets the total time allowed for a particular remediation process. When the interval is set to 0, the Agent continues to attempt Auto Remediation until the temporary role times out.
  - **AV Definition Update/AS Definition Update/Windows Server Update Services**—when the initial remediation attempt fails, this interval defines how long the Agent waits before it restarts the next update attempt. For example, if setting this interval to 30 seconds for an AV Definition Update, at the end of the initial attempt to update the client's AV definition file, the Agent waits 30 seconds then starts the next update attempt if the requirement failed.
  - **Link Distribution/Windows Update/Launch Programs**—for these requirement types, the interval defines the total number of seconds the Agent allows for the remediation attempt to complete. For example, if setting this interval to 60 seconds for a Launch Programs requirement, the Agent launches the program(s) and allows 60 seconds for the programs to execute. If the client has not met the requirement at the end of 60 seconds, the Agent launches the programs again immediately.

Step 5 Enter a value for the **Retry Count []**:

- **Retry Count []** - Default is 0. When the interval is 0, the Agent continues to attempt Auto Remediation until the temporary role times out. Otherwise, specifying a retry count sets a limit on the number of times the Agent automatically retries the requirement if it initially fails. If the Retry Count is reached before the Temporary role timeout, the Auto Remediation dialog displays red status text telling the user to click the **Manual** button.
  - **AV Definition Update / AS Definition Update / Windows Server Update Services**
  - **Link Distribution / Windows Update / Launch Programs**

If a Mandatory requirement still fails after the Retry Count, the Agent stops and does not perform the next priority requirement for the user role. Users will not have network access.

For an Optional requirement, the Agent always continues to the next requirement after the initial attempt finishes, regardless of the Retry Count specified and whether the initial attempt succeeded or failed. However, if an Interval is specified, the Agent waits that amount of time before continuing to the next requirement.

If Auto Remediation fails, the user receives a failure message and can click the **Details** button to view the remediation results, or click **Continue** to return to the Clean Access Agent authentication process. The user can then either cancel the login session or accept "restricted" network access.

Post-Configuration and Agent Maintenance on the CAM

Once you have configured Agent login and client posture assessment, and users are able to successfully access the Cisco NAC Appliance network, you can use the following topics to manage Agent versions on client machines in your network:

- Manually Uploading the Agent to the CAM, page 9-100
- Downgrading the Agent, page 9-101
- Configure Agent Auto-Upgrade, page 9-102

Note If you are uploading an older (pre-release 4.6(1) Windows Clean Access Agent to the CAM, refer to the uploading and downgrading instructions in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)*.

Manually Uploading the Agent to the CAM

When performing a software upgrade or new install of the CAM/CAS, it is not necessary to upload Agent installation files since they are automatically included with the CAM software. In certain cases, you can manually upload either the Windows Cisco NAC Agent Installation File (nacagentsetup-win.tar.gz) or Mac OS X Agent Installation File (CCAAgentMacOSX-4.9.x.y-k9.tar.gz) directly to the CAM (for example, if you need to reinstall the Agent or downgrade the version of the Agent distributed to new users—see Downgrading the Agent, page 9-101 for details).

To support Windows Clean Access Agent backward compatibility, you can also manually upload the Windows Clean Access Agent Setup File (CCAAgentSetup-4.x.y.z.tar.gz) directly to the CAM. This feature allows administrators to revert to a previous Windows Agent Setup file for distribution. You can manually upload the Agent Setup File using the CAM **Device Management > Clean Access > Clean Access Agent > Distribution** web console page.

Note The CAM will automatically publish the Agent Installation/Setup file to the connected CAS(s) when the file is uploaded manually. There is no version check while publishing, so the Agent Installation/Setup can be downgraded or replaced. For details on version compatibility for the CAM/CAS and Agent, refer to *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.

Caution You must upload the Agent file as a **tar.gz** file (without untarring it) to the CAM. Make sure you do NOT extract the .exe file before uploading.

Step 1 Log in to the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. You will likely be required to provide your CCO credentials.

Step 2 Choose **Security > Endpoint Security > Cisco Network Access Control > Cisco NAC Appliance > Cisco NAC Appliance 4.9**.

Step 3 Click the directory link for the appropriate release, for example “4.9.5.”

Step 4 Download the Cisco NAC Agent (nacagentsetup-win.tar.gz) installer file to your local machine.

Note The CAM does not accommodate Cisco NAC Agent installation files (nacagentsetup-win.tar.gz) and Windows Clean Access Agent Setup files (CCAAgentSetup-4.x.y.z.tar.gz) simultaneously. If you upload an older Windows Clean Access Agent Setup file, you will wipe out the existing Cisco NAC Agent installation and XML Agent configuration files, and vice-versa.

Step 5 Go to **Device Management > Clean Access > Clean Access Agent > Distribution** (see Agent Distribution, page 9-18).

Step 6 In the **Upload Agent File** field, click **Browse**, and navigate to the folder where the appropriate Agent file is located.

Step 7 Select the .tar.gz file and click **Open**. The name of the file should appear in the text field.

Step 8 In the **Version** field, type the version of the Agent to be uploaded.

Caution You must upload the Agent file as a **tar.gz** file (without untarring it) to the CAM. Make sure you do NOT extract the .exe file before uploading.

Step 9 Click **Upload**.

Downgrading the Agent

The following steps describe how to manually downgrade the version of the Agent on the CAM.

Step 1 Under **Device Management > Clean Access > Clean Access Agent > Distribution**, disable the **Current NAC Agent is a mandatory upgrade** checkbox and click **Update**.

Step 2 Under **Device Management > Clean Access > Updates**, disable the **Check for Windows NAC Agent updates** checkbox and click **Update**.

Step 3 Follow the instructions in Manually Uploading the Agent to the CAM, page 9-100.

Note Users cannot automatically “downgrade” the Cisco NAC Agent on the client machine. In order to support Agent downgrade for the Cisco NAC Agent, the user must first uninstall the existing Agent, then log back into Cisco NAC Appliance to install the available Agent version.

Step 4 Make sure that all the CASs are listed with a status of “Connected” under **Device Management > CCA Servers > List of Servers**.

Step 5 Under **Device Management > Clean Access > Clean Access Agent > Distribution**, browse to and upload first the Setup.tar.gz file to the CAM. Make sure you type the correct version of the Agent (for example, “4.1.10.0”) in the **Version** field before you click **Upload**. Files will be published to the CASs automatically.

Note The CAM does not accommodate Cisco NAC Agent installation files (nacagentsetup-win.tar.gz) and Windows Clean Access Agent Setup files (CCAAgentSetup-4.x.y.z.tar.gz) simultaneously. If you upload an older Windows Clean Access Agent Setup file, you will wipe out the existing Cisco NAC Agent installation and XML Agent configuration files, and vice-versa.

Step 6 Create a Local Check requirement that provides instructions to the end user to uninstall the Agent (e.g. 4.1.x.y) and perform weblogin again to download the downgraded Agent (e.g. 4.1.2.1).

Note The Mac OS X Agent does not support downgrade. For example, if you upload an old Mac OS X Agent (lower version number) and check the **Current NAC Agent is a mandatory upgrade** option, the client machine does not prompt for auto-upgrade.

Configure Agent Auto-Upgrade

This section describes the following:

- Enable Agent Auto-Upgrade on the CAM, page 9-102
- Disable Agent Upgrades to Users, page 9-102
- Disable Mandatory Agent Auto-Upgrade on the CAM, page 9-103
- User Experience for Agent Auto-Upgrade, page 9-103
- Uninstalling the Agent, page 9-103
- Agent Auto-Upgrade Compatibility, page 9-106

Enable Agent Auto-Upgrade on the CAM

To enable Agent Auto-Upgrade, you must:

- Be running Cisco NAC Appliance release 4.1(0) or later on the Clean Access Manager and Clean Access Server, and already have the Agent installed on client machines. (See User Experience for Agent Auto-Upgrade, page 9-103.)
- Require use of the Agent for the role and client operating system. (See Require Agent Login for Client Machines, page 9-3.)
- Retrieve the latest version of the Agent installation file. For both mandatory or optional Auto-Upgrade, a newer version of the Agent installer must be downloaded to the CAM via **Device Management > Clean Access > Updates > Update**, or users will not be prompted to upgrade to the newer Agent. (See Require Agent Login for Client Machines, page 9-3.)

Note If you have upgraded the Cisco NAC Web Agent installer, users logging in using the Web Agent always log in using that Agent version.

Disable Agent Upgrades to Users

You can disable notification and distribution of the Agent installation file upgrade to users as follows:

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Distribution** (see Figure 9-6 on page 9-18).

Step 2 Enable (check) the **Do not offer current NAC Agent to users for upgrade** option.

Step 3 Click **Update**.

Disable Mandatory Agent Auto-Upgrade on the CAM

New installs of the CAM/CAS automatically enable mandatory auto-upgrade by default. For CAM/CAS upgrades, the current setting (enabled or disabled) will be carried over to the upgraded system. To disable mandatory Agent auto-upgrade for all users:

Step 1 Go to **Device Management > Clean Access > Clean Access Agent > Distribution** (Figure 9-6 on page 9-18).

Step 2 Disable (uncheck) the **Current NAC Agent is a mandatory upgrade** option.

Step 3 Click **Update**.

Note Cisco recommends setting the **Current NAC Agent is a mandatory upgrade** option to ensure the latest AV/AS product support.

User Experience for Agent Auto-Upgrade

With auto-upgrade enabled, and a newer version of the Agent available in the CAM, the user experience is as follows:

- New users download and install the latest available version of the Agent after the initial one-time web login.
- Existing users are prompted at login to auto-upgrade to the latest version of the Agent available (if upgrade notification is enabled for users). After the user accepts the prompt to upgrade, the client automatically begins installing the newer Agent version.
- Out-of-Band users must be on the Authentication VLAN to be prompted to automatically upgrade the Agent at login.
- In-Band users remain logged into the Agent when the user logs off the Windows domain or shuts down the machine, unless the **General Setup** page is configured otherwise. See Logoff NAC Agent users from network on their machine logoff or shutdown after <x> secs (for Windows & In-Band setup, for OOB setup when OOB Logoff is enabled), page 1-10 for details.

Uninstalling the Agent

This section describes how to:

- Uninstall Cisco NAC Agent, page 9-104
- Uninstall Windows Clean Access Agent, page 9-104
- Uninstall Mac OS X Agent, page 9-104

Uninstall Cisco NAC Agent

The Agent installs to **C:\Program Files\Cisco\Cisco NAC Agent** on the Windows client. You can uninstall the Agent in the following ways:

- By double-clicking the **Uninstall Cisco NAC Agent** desktop icon
- By going to **Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Cisco NAC Agent**
- By going to **Start Menu > Control Panel > Add or Remove Programs > Cisco NAC Agent**

Note To change the version of the Agent on the CAM, see Manually Uploading the Agent to the CAM, page 9-100.

To uninstall Cisco NAC Agent in a Windows 8 client, execute the following:

Step 1 Switch to Metro Mode.

Step 2 Right-Click **Cisco NAC Agent** tile.

Step 3 Select **Un-Install** from the options available at the bottom of the screen.

Step 4 The system automatically switches to Desktop mode and opens **Add/Remove** control panel.

Step 5 In the **Add/Remove** control panel, perform one of the following:

- Double Click **Cisco NAC Agent**.
- Select **Cisco NAC Agent** and click **Uninstall**.
- Right Click **Cisco NAC Agent** and select **Uninstall**.

Uninstall Windows Clean Access Agent

The Agent installs to C:\Program Files\Cisco Systems\Clean Access Agent\ on the Windows client. You can uninstall the Clean Access Agent in the following ways:

- By going to **Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Clean Access Agent**
- By going to **Start Menu > Control Panel > Add or Remove Programs > Cisco Clean Access Agent**

Note To change the version of the Agent distributed from the CAM, see Manually Uploading the Agent to the CAM, page 9-100.

Uninstall Mac OS X Agent

In Mac OS X Agent version 4.8.2.590 and later, you can uninstall the Agent by running the uninstall script as follows:

Step 1 Open the navigator pane and navigate to *<local drive ID>* > **Applications**.

Step 2 Highlight and right-click the **CCAAgent** icon to bring up the selection menu.

Step 3 Choose **Show Package Contents** and double-click **NacUninstall.**

Step 4 This will uninstall the Agent on Mac OS X.

In the previous versions of Mac OS X Agent, there are two steps to uninstall the Agent:

Step 1 Perform any one of the following:

- Open up a Terminal.app session and enter the following:

```
sudo rm -rf /sbin/dhcp_refresh /opt/cisco/nac/Applications/CCAAgent.app
```

[or]

- For Mac OS X 10.7, open up a Terminal.app session and enter the following:

```
sudo rm -rf /sbin/dhcp_refresh /Applications/CCAAgent.app
```

[or]

- Drag the Agent application to the trash can. The Agent application is located at **/Library/Application Support/Cisco Systems/CCAAgent.app.**
- For Mac OS X 10.7, go to **Finder > Application > CCAAgent.app**, right-click and then click **Move to Trash**.

Step 2 For Mac OS X 10.5, enter the following in the Terminal.app session:

```
sudo rm -rf /Library/Receipts/CCAAgent.pkg
```

For Mac OS X 10.6 and 10.7, enter the following in the Terminal.app session:

```
sudo rm -rf /var/db/receipts/com.cisco.cca.CCAAgent.*
```

Once these two steps are done, the next time you run the installer, the button in the installer will display "INSTALL" instead of "UPGRADE" because you have completely removed all traces of the application.

Removing the dhcp_refresh Tool from Macintosh OS X

To completely remove the Mac OS X Agent and related files, you must ensure that the **dhcp_refresh** file under /sbin folder is deleted.

You may need to manually remove the **dhcp_refresh** tool that is copied and stored in **/sbin**. The **dhcp_refresh** tool is copied to this location in two ways—it is copied using either the Java applet or **Macagent** installer applications. There are two ways you can remove this tool:

- Open up a **Terminal.app** session and enter the following:

```
cd /sbin
sudo rm dhcp_refresh
```

- Use the **Finder.app** method:
  a. Navigate to **Finder > Go > Go to Folder**.
  b. Enter **/sbin** at the prompt.
  c. Drag the **dhcp_refresh** file to the trash can.
  d. Enter your administrator password at the authentication dialog that pops up.

Agent Auto-Upgrade Compatibility

The newest version of the Agent installation files are automatically included with the CAM software for each Cisco NAC Appliance software release. Every version of the Agent is compatible with the same version of the server product. For example:

- 4.9.5.6 Cisco NAC Agent works with 4.9(5) CAS/CAM

By design, every new 4.9.5.x Agent is intended to have basic backward compatibility with any 4.8(x) Clean Access Server. In addition, 4.9(5) Clean Access Servers are designed to be compatible with Agent 4.9.4.x and later. Basic compatibility means, the Agent is able to perform basic functions such as login, logout, look for configured requirements, and report vulnerabilities.

For Clean Access Agent version compatibility details, see *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.

Versioning

The Cisco NAC Agent uses 4-digit versioning:

- Cisco NAC Agent version 4.9.5.6 is bundled with Cisco NAC Appliance Release 4.9(5).
- Upgrades to the Agent (e.g. 4.9.5.x) typically correspond to AV/AS product support enhancements and/or Agent compatibility (e.g. OS support).

New Agent versions bundled with a Cisco NAC Appliance release (e.g. Cisco NAC Agent version 4.9.0.33) incorporate and supersede previous versions of the Clean Access Agent (e.g. 4.8.x.y).

Cisco Updates

With auto-upgrade enabled and the Agent already installed on clients, the Agent automatically detects when an Agent update is available, downloads the update from the CAS, and upgrades itself on the client after user confirmation. Administrators can make Agent auto-upgrade mandatory or optional for users.

To prevent distribution of the Agent update to users altogether, you can check the **Do not offer current NAC Agent to users for upgrade** option from the Agent **Distribution** page. This prevents the user upgrade notification when a newer Agent update becomes available on the CAM.

Note For further details on version upgrade restrictions, refer to the "Agent Upgrade Compatibility Matrix" of the corresponding *Release Notes for Cisco NAC Appliance*.



Cisco NAC Appliance Agents

This chapter presents overviews, login flow, and session termination dialogs for the following Cisco NAC Appliance access portals:

- Cisco NAC Agent, page 10-1
- Cisco NAC Web Agent, page 10-25
- Mac OS X Cisco NAC Agent, page 10-44

Note For details on the Windows versions of the Clean Access Agent that are still supported in release 4.9(5), refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.9(x)* and the corresponding *Release Notes for Cisco NAC Appliance*.

Cisco NAC Agent

This section describes how to configure the Cisco NAC Agent to allow users to log in to the internal network via a persistent network access application installed on the client machine.

- Windows Cisco NAC Agent Overview, page 10-1
- Configuration Steps for the Windows Cisco NAC Agent, page 10-3
- Windows Cisco NAC Agent User Dialogs, page 10-3

Windows Cisco NAC Agent Overview

The Cisco NAC Agent provides local-machine Agent-based posture assessment and remediation for client machines. The Cisco NAC Agent is designed to provide user login capability on a wide range of Windows client machines, including clients running 64-bit operating systems, and offers “double-byte” support to enable native localization for a large variety of languages.

Users download and install the Cisco NAC Agent (read-only client software), which can check the host registry, processes, applications, and services. The Cisco NAC Agent can be used to perform Windows updates or antivirus/antispyware definition updates, launch qualified remediation programs, distribute files uploaded to the Clean Access Manager, distribute website links to websites in order for users to download files to fix their systems, or simply distribute information/instructions.

Users without administrator privileges upgrading their Windows client machine from an earlier version of the Clean Access Agent (version 4.5.2.0 or 4.1.10.0 and earlier) to the Cisco NAC Agent must have the **CCAAgentStub.exe** Agent Stub installed on the client machine to facilitate upgrade. (Users with

administrator privileges do not need this file.) After successful Cisco NAC Agent installation, the user is not required to have administrator privileges on the client machine, nor is the **CCAAgentStub.exe** Agent Stub file needed.

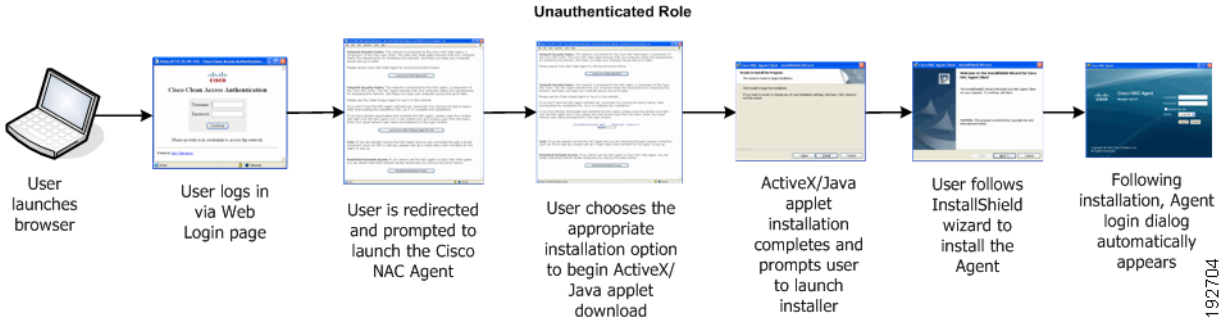
After users log into the Cisco NAC Agent, the Agent gets the requirements configured for the user role/operating system from the Clean Access Server, checks for the required packages, and sends a report back to the CAM (via the CAS). If requirements are met on the client, the user is allowed network access. If requirements are not met, the Agent presents a dialog to the user for each unmet requirement. The dialog (configured in the New Requirement form) provides the user with instructions and the action to take for the client machine to meet the requirement.

Cisco NAC Agent posture assessment is configured in the CAM by creating requirements based on rules and (optionally) checks, then applying the requirements to user roles/client operating systems. For more information, see Configuring Agent-Based Posture Assessment, page 9-39.

Cisco NAC Agent Download

Figure 10-1 illustrates the general user sequence for the initial download and install of the Cisco NAC Agent, if the administrator has required use of the Agent for the user's role and OS.

Figure 10-1 Downloading the Cisco NAC Agent


Unauthenticated Role
User launches browser
User logs in via Web Login page
User is redirected and prompted to launch the Cisco NAC Agent
User chooses the appropriate installation option to begin ActiveX/ Java applet download
ActiveX/Java applet installation completes and prompts user to launch installer
User follows InstallShield wizard to install the Agent
Following installation, Agent login dialog automatically appears
192704

The Cisco NAC Agent software is always included as part of the Clean Access Manager software. When the CAM is installed, the Agent Installation file is already present and automatically published from the CAM to the CASs. To distribute the Agent to clients, you simply require the use of the Agent in the CAM web console for the desired user role/operating system. Once downloaded and installed, the Agent performs checks on the client according the requirements you have configured in the CAM.

First-time users can download and install the Agent by opening a web browser to log into the network. If the user's login credentials associate the user to a role that requires the Agent, the user will be redirected to the Agent download page. After the Agent is downloaded and installed, the user is immediately prompted to log into the network using the Agent dialogs, and is scanned for requirements. After successfully meeting the requirements configured for the user's role and operating system and passing scanning (if enabled), the user is allowed access to the network.

Note In Windows 8 Operating System, the Internet Explorer has two modes, Desktop and Metro. In the Metro mode, the ActiveX plugins are restricted. You cannot download NAC Agent in the Metro mode. You must switch to Desktop mode and then launch Internet Explorer to download NAC Agent.

Note Unlike the Clean Access Agent, the Cisco NAC Agent does not support Nessus-based network scanning.

You can distribute Agent Upgrades to clients by configuring auto-upgrade options in the web console. Agent Upgrades are retrieved on the CAM via Retrieving Cisco NAC Appliance Updates, page 9-12.

Configuration Steps for the Windows Cisco NAC Agent

The basic steps needed to configure the Windows Cisco NAC Agent are as follows:

1. Make sure to follow the steps in Agent Configuration Steps, page 9-3 to enable distribution and download of the Cisco NAC Agent.
2. Configure Agent requirements using the instructions in Configuring Agent-Based Posture Assessment, page 9-39:
   a. Configuring AV/AS Definition Update Requirements, page 9-41
   b. Configuring a Windows Server Update Services Requirement, page 9-57
   c. Configuring a Windows Update Requirement, page 9-64
   d. Configuring Custom Checks, Rules, and Requirements, page 9-70
   e. Configuring a Launch Programs Requirement, page 9-85
   f. Map Requirements to Rules, page 9-90
   g. Apply Requirements to User Roles, page 9-92
   h. Validate Requirements, page 9-93
   i. Configuring an Optional/Audit Requirement, page 9-94

Windows Cisco NAC Agent User Dialogs

Note Client machine browsers accessing a FIPS-compliant Cisco NAC Appliance network require TLSv1 in order to "talk" to the network, which is disabled by default in Microsoft Internet Explorer Version 6. Users can enable this option in Internet Explorer version 6 by following the same instructions for administrators accessing the CAM/CAS web console via IE version 6. See the "Enabling TLSv1 on Internet Explorer Version 6" installation troubleshooting section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

This section illustrates the user experience when Cisco NAC Appliance is installed on your network and the Cisco NAC Agent is required and configured for the user role.

Note For details on the Cisco NAC Agent when configured for Single Sign-On (SSO) behind a VPN concentrator, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

1. When the user first opens a web browser, the user is redirected to the web login page (Figure 10-36).

Figure 10-2 Login Page



2. The user logs into the web login page and is redirected to the Agent Download page (Figure 10-3) for the one-time download of the Cisco NAC Agent installation file.

Figure 10-3 Cisco NAC Agent Download Page

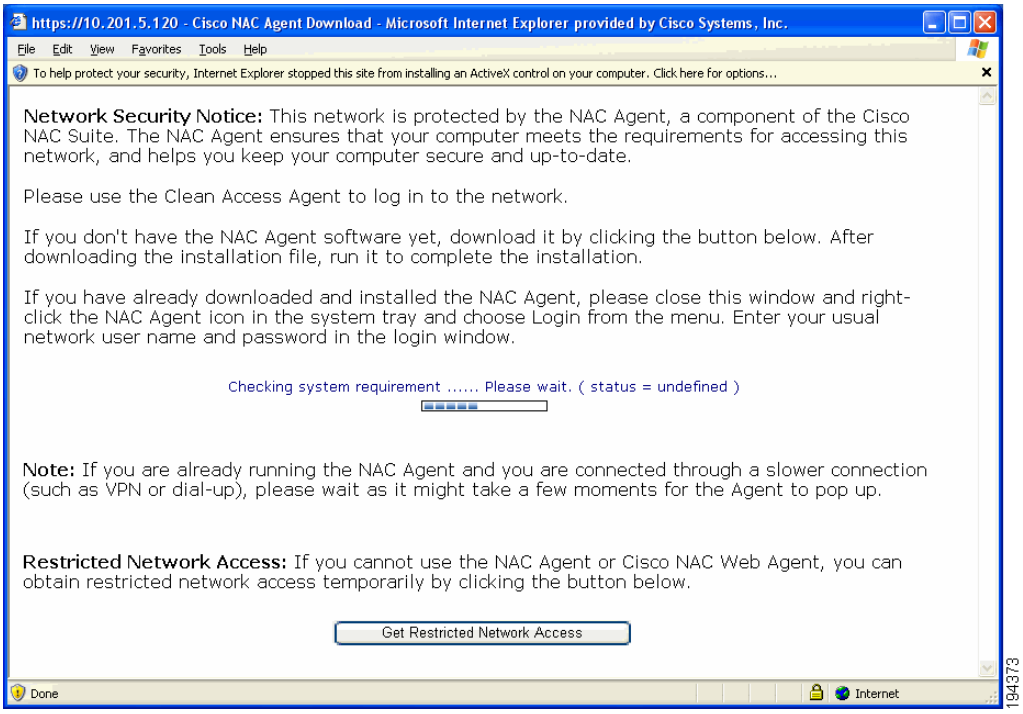

Cisco NAC Web Agent Download
Page
Safety
Tools
Network Security Notice: This network is protected by a Cisco NAC Appliance Agent, a component of the Cisco NAC Appliance Suite. The Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please use the Agent to log in to the network.
If you don't have the Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.
If you have already downloaded and installed the Agent, please close this window and right-click the Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.
Launch Cisco NAC Windows Agent 4.9.5.6
Note: If you are already running the NAC Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the

3. The user clicks the **Launch Cisco NAC Windows Agent Installer** button (the button displays the version of the Agent being downloaded).

Note If the **Allow restricted network access in case user cannot use Cisco NAC Agent or Cisco NAC Web Agent** option is selected under **Device Management > Clean Access > General Setup > Agent Login**, the **Get Restricted Network Access** button and related text will display in the Agent Download page. See Agent Login, page 1-7 for details.

Note If the existing CAS certificate is not trusted on the client, the user must accept the optional certificate in the **Security Alert** dialog that appears before the user can download the Agent.

Figure 10-4 ActiveX Installation Notice

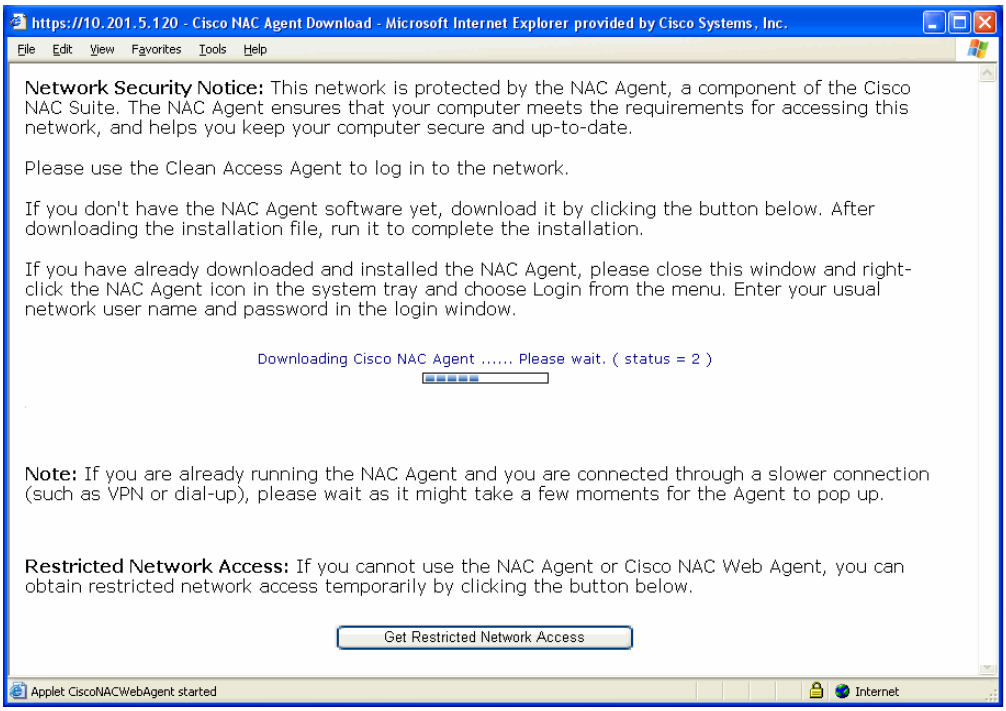

https://10.201.5.120 - Cisco NAC Agent Download - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
To help protect your security, Internet Explorer stopped this site from installing an ActiveX control on your computer. Click here for options...
Network Security Notice: This network is protected by the NAC Agent, a component of the Cisco NAC Suite. The NAC Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please use the Clean Access Agent to log in to the network.
If you don't have the NAC Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.
If you have already downloaded and installed the NAC Agent, please close this window and right-click the NAC Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.
Checking system requirement ..... Please wait. (status = undefined)
Note: If you are already running the NAC Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the Agent to pop up.
Restricted Network Access: If you cannot use the NAC Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Done
Internet
194373

4. If the user's web browser settings are configured to verify actions like installing an ActiveX control on the client machine, the user may need to verify the action. For example, in the case of Microsoft IE, the user may need to click on a status bar that appears in the browser window and choose the **Install ActiveX Control** option from the resulting pop-up to validate the ActiveX process. If the ActiveX control fails to initialize, the user sees an ActiveX installation notice and, if you have set up the Cisco NAC Appliance system to do so, the Cisco NAC Appliance system attempts to download the Agent installation files via Java applet.

Note ActiveX is supported only on the 32-bit versions of Internet Explorer. You cannot install ActiveX on a Firefox web browser or on a 64-bit version of Internet Explorer.

Note If you specify that the Java applet method is preferred using the **Web Client (ActiveX/Applet)** option in the **Administration > User Pages > Login Page** configuration screen, the order of these possibilities is reversed—the user sees a Java applet failure notice before the ActiveX control attempts to install the Agent files on the client machine.

Figure 10-5 Java Installation Notice


https://10.201.5.120 - Cisco NAC Agent Download - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Network Security Notice: This network is protected by the NAC Agent, a component of the Cisco NAC Suite. The NAC Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please use the Clean Access Agent to log in to the network.
If you don't have the NAC Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.
If you have already downloaded and installed the NAC Agent, please close this window and right-click the NAC Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.
Downloading Cisco NAC Agent ..... Please wait. (status = 2)
Note: If you are already running the NAC Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the Agent to pop up.
Restricted Network Access: If you cannot use the NAC Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Applet CiscoNACWebAgent started
Internet
194374

Note If the version of the Agent being downloaded from the CAM is "unsigned" (if it has been handed over directly from Cisco Support as a patch version, for example), the user may see an additional Java Security Notice like the one in Figure 10-6.

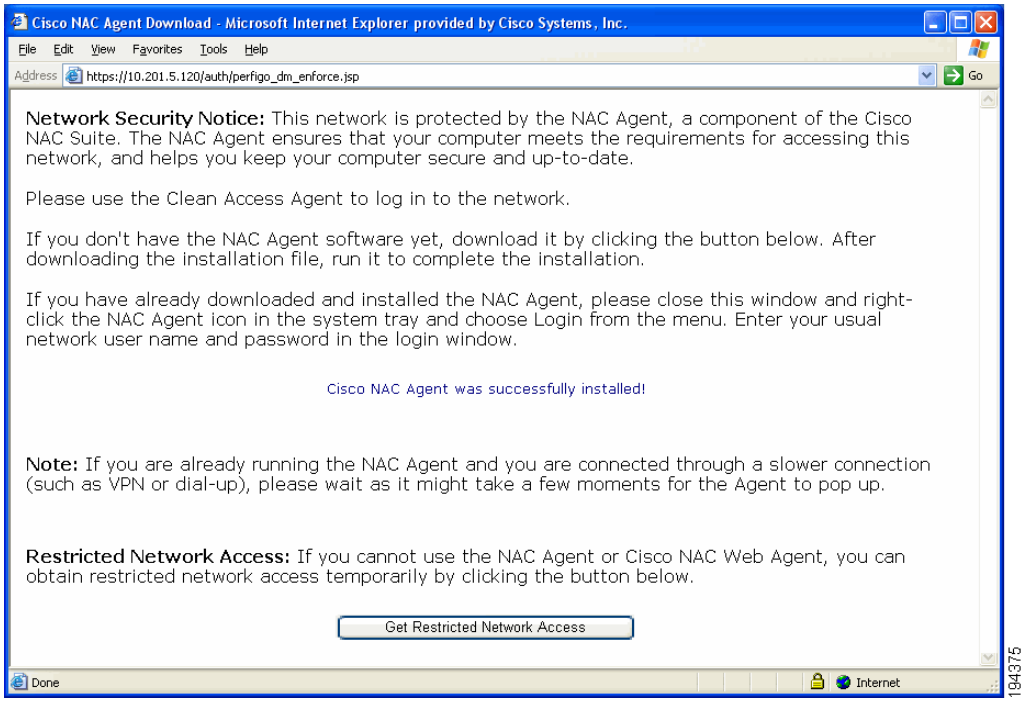
Figure 10-6 Java Applet Security Notice


Warning - Security
Do you want to accept the certificate from web site "10.201.5.120" for the purpose of exchanging encrypted information?
Publisher authenticity verified by: "Perfigo, Inc."
The security certificate was issued by a company that is not trusted.
The security certificate has not expired and is still valid.
Caution: "10.201.5.120" asserts that this content is safe. You should only accept this content if you trust "10.201.5.120" to make that assertion.
More Details
Yes
No
Always
185979

If both the ActiveX and Java applet Agent download and install methods fail, the user sees a Windows dialog informing the user that Cisco NAC Agent login failed and must either contact the Cisco NAC Appliance network administrator to try and help troubleshoot issues with the installation process, or (if enabled for the user's login role) accept "Restricted" network access for the time being until they can fix the Agent installation problem.

5. After the user allows the ActiveX control to install the Agent files or acknowledges the Java certificate security warning and chooses to accept the Java applet contents, the client machine goes to work downloading the Agent installer and all required ancillary files and saving them on the client machine and the browser window displays a "Cisco NAC Agent was successfully installed!" message (Figure 10-7).

Figure 10-7 Cisco NAC Agent Installed Successfully


Cisco NAC Agent Download - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Address https://10.201.5.120/auth/perfigo_dm_enforce.jsp
Go
Network Security Notice: This network is protected by the NAC Agent, a component of the Cisco NAC Suite. The NAC Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please use the Clean Access Agent to log in to the network.
If you don't have the NAC Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.
If you have already downloaded and installed the NAC Agent, please close this window and right-click the NAC Agent icon in the system tray and choose Login from the menu. Enter your usual network user name and password in the login window.
Cisco NAC Agent was successfully installed!
Note: If you are already running the NAC Agent and you are connected through a slower connection (such as VPN or dial-up), please wait as it might take a few moments for the Agent to pop up.
Restricted Network Access: If you cannot use the NAC Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Done
Internet
194375

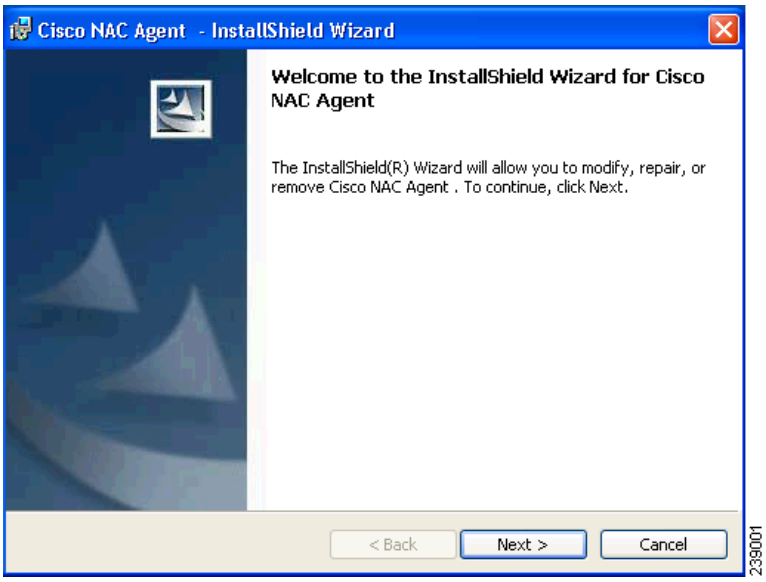
The installation step in the process can take anywhere from just a few seconds to several minutes, depending on your connection speed. Typically, a fast connection speed like a 10/100 Ethernet LAN link will take very little time, whereas a relatively slow connection link like ISDN could take significantly longer.

6. The user should **Save** the Update.exe file to a download folder and then **Run** the executable on the client machine.

Note If the CAS certificate is not trusted on the client, the user must accept the certificate in the **Security Alert** dialog that appears before Agent installation can successfully proceed.

7. The **Cisco NAC Agent Client - Welcome to the InstallShield Wizard** dialog appears (Figure 10-8).

Figure 10-8 Cisco NAC Agent InstallShield Wizard—Welcome


Cisco NAC Agent - InstallShield Wizard
Welcome to the InstallShield Wizard for Cisco NAC Agent
The InstallShield(R) Wizard will allow you to modify, repair, or remove Cisco NAC Agent . To continue, click Next.
< Back
Next >
Cancel
239001

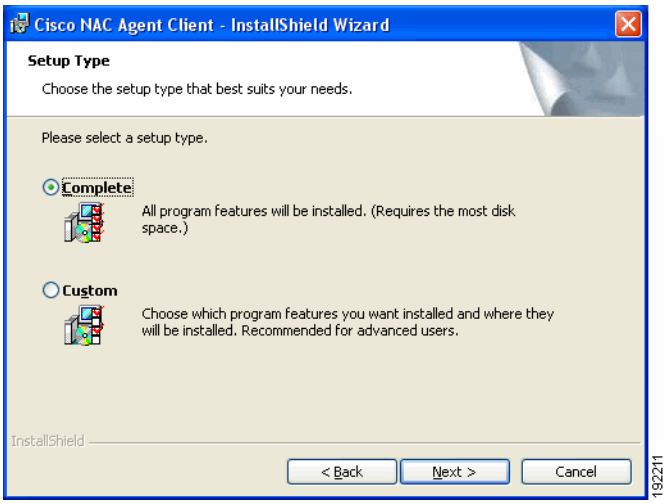
8. Before the Agent installation process can continue, the user must first click the **I accept the terms in the license agreement** option in the "End User License Agreement" dialog and click **Next** (Figure 10-9).

Figure 10-9 Cisco NAC Agent Installation—License Agreement


Cisco NAC Agent - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
End User License Agreement
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel
192676

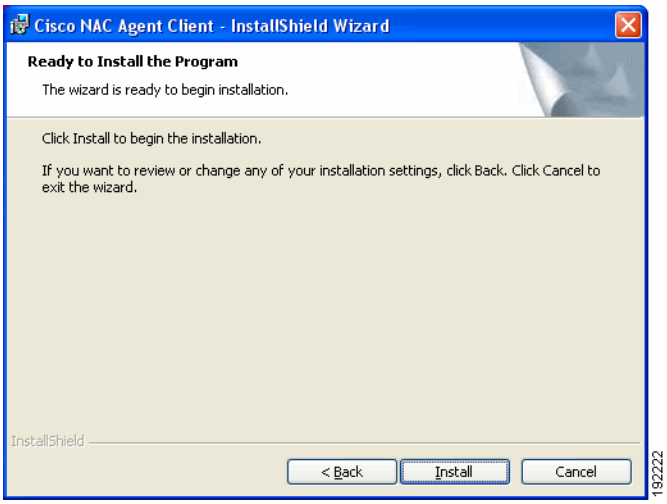
9. The user also has the option to install the complete collection of Cisco NAC Agent files or specify one or more items by choosing the **Custom** option and clicking **Next** (Figure 10-10).

Figure 10-10 Cisco NAC Agent Installation—Setup Type


Cisco NAC Agent Client - InstallShield Wizard
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel
192211

10. The **Cisco NAC Agent Client - InstallShield Wizard** dialog appears (Figure 10-11).

Figure 10-11 Cisco NAC Agent InstallShield Wizard—Ready to Install


Cisco NAC Agent Client - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel
192222

11. The setup wizard prompts the user through the short installation steps to install the Cisco NAC Agent to **C:\Program Files\Cisco\Cisco NAC Agent**.

Figure 10-12 Cisco NAC Agent Installation In Progress

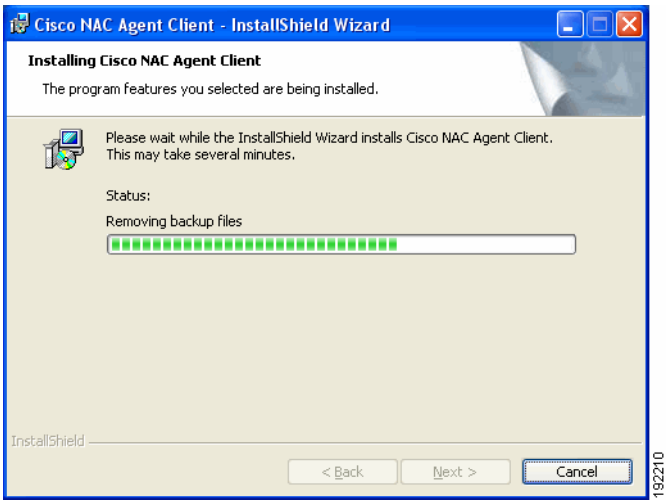
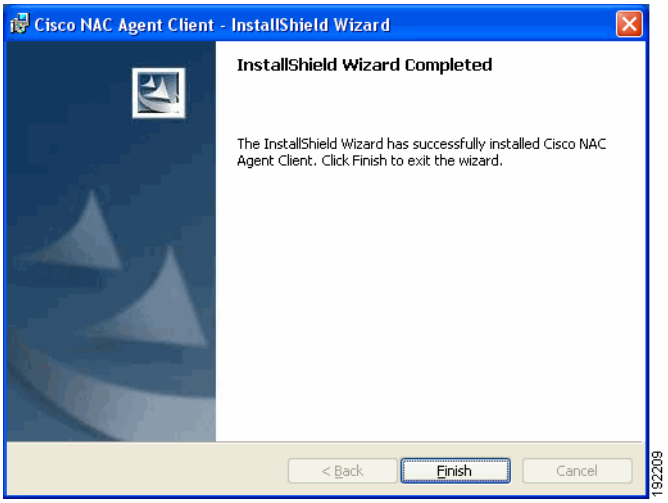
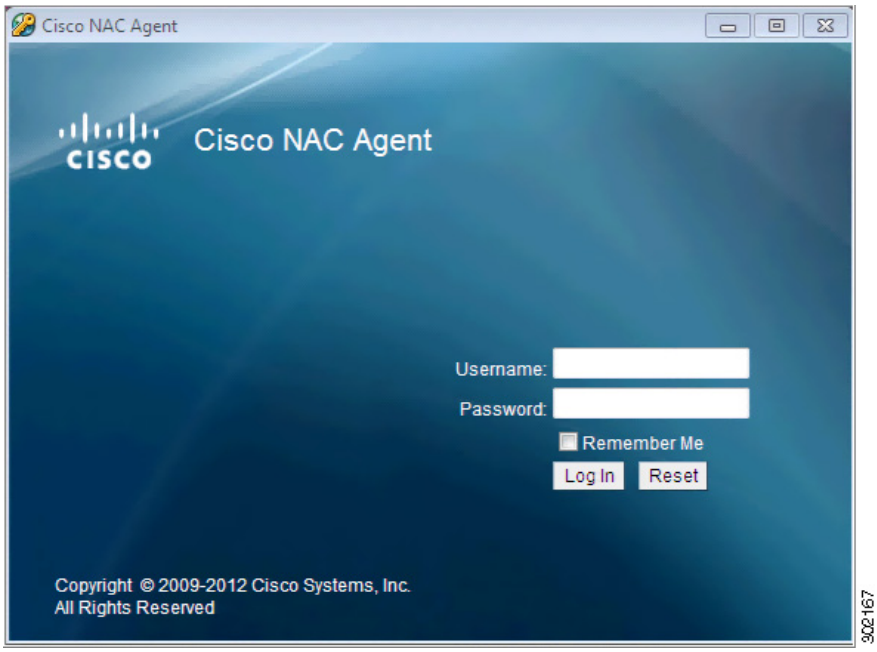

Cisco NAC Agent Client - InstallShield Wizard
Installing Cisco NAC Agent Client
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Cisco NAC Agent Client. This may take several minutes.
Status:
Removing backup files
InstallShield
< Back
Next >
Cancel
192210

Figure 10-13 Cisco NAC Agent Installation Complete


Cisco NAC Agent Client - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Cisco NAC Agent Client. Click Finish to exit the wizard.
< Back
Finish
Cancel
192209

12. When the InstallShield Wizard completes and the user clicks **Finish**, the Cisco NAC Agent login dialog pops up (Figure 10-14) and the Cisco NAC Agent taskbar icon appears in the system tray.

Figure 10-14 Cisco NAC Agent Login Dialog



13. The user enters credentials to log into the network. Similar to the web login page, the user can choose an authentication provider from the **Server** list (if configured for multiple authentication providers).

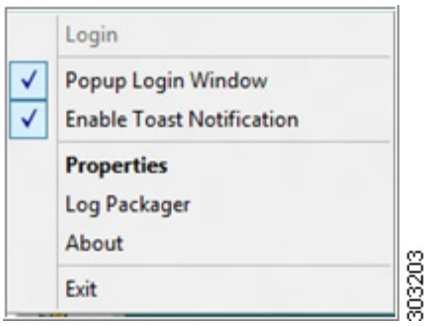
Note If multiple authentication providers are available in the **Server** list, when a user logs in with invalid credentials, the Server automatically changes to the default authentication provider. Checking the session-based **Remember Me** checkbox causes to show the last selected provider instead of default authentication server, in case of invalid credentials.

Note Clicking the session-based **Remember Me** checkbox causes the **User Name** and **Password** fields to be populated with the last values entered throughout multiple logins/logouts if the user does not exit or upgrade the application or reboot the machine. On shared machines, the **Remember Me** checkbox can be unchecked to ensure multiple users on the machine are always prompted for their individual username and password.

If Cisco NAC Appliance employs a RADIUS server for user authentication and the server has been configured to authenticate users with additional credentials, the user may be presented with one or more additional challenge-response dialogs like those described in RADIUS Challenge-Response Cisco NAC Agent Dialogs, page 10-22.

14. The user can right-click the Cisco NAC Agent icon in the system tray to bring up the taskbar menu for the Agent (Figure 10-15).

Figure 10-15 Cisco NAC Agent Taskbar Menu



Taskbar menu options are as follows:

Login/Logout—This toggle reflects the login status of the user. **Login** means the user is behind a Clean Access Server and is not logged in. **Logout** means the user is already logged into Cisco NAC Appliance. **Disabled (grey) Login** occurs when there is no SWISS response from the CAS to the Cisco NAC Agent. This condition is expected in the following cases:

- The Cisco NAC Agent cannot find a Clean Access Server or the Agent is logged in, but has lost contact with the CAS.
- OOB deployments: the Cisco NAC Agent user has already logged in through the CAS and is now on the Access VLAN.
- Multi-hop Layer 3 (VPN/WLC) deployments with SSO: the user has authenticated through the VPN concentrator and therefore is already automatically logged into Cisco NAC Appliance.
- Device Filters: MAC address-based authentication is configured for the machine of this user and therefore no user login is required.

Popup Login Window—This option is set by default when the Cisco NAC Agent is first installed and causes the Agent login dialog to automatically pop up when it detects that the user is behind a Clean Access Server and is not logged in.

Enable Toast Notification—This option is available only for clients using Windows 8 as Operating System. You can enable this option to send relevant notifications to the user. See Windows 8 Metro and Metro App Support —Toast Notifications, page 10-13 for more details.

Log Packager—Click this option to run the support package and collect the logs. This option is available only starting from Cisco NAC Appliance Release 4.9(1).

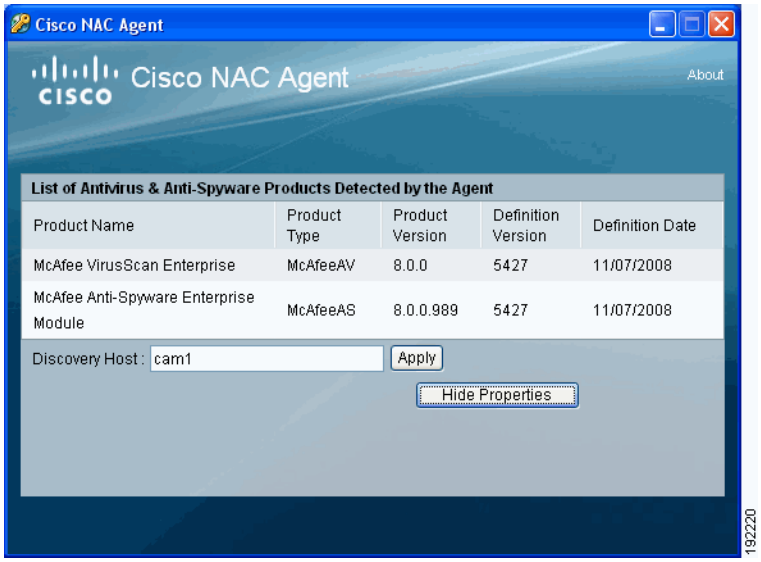
Properties—Selecting **Properties** brings up the **Agent Properties and Information** dialog (Figure 10-16) which shows all of the AV and AS products installed on the client machine and the Discovery Host for Layer 3 deployments.

You can access the above options by using the keyboard shortcuts as follows:

- L — Login/Logout
- A — About
- X — Exit
- R — Properties
- P — Popup Login Window

Note The Discovery Host field can be made editable by changing the **DiscoveryHostEditable** parameter in the Agent configuration XML file. See Cisco NAC Agent XML Configuration File Settings, page 9-23 for more details.

Figure 10-16 Properties



About—Displays the version of the Cisco NAC Agent.

Exit—Exits the application, removes the Cisco NAC Agent icon on the taskbar, and automatically logs off the users in both In-Band and Out-of-Band mode. The users in Out-of-Band mode are logged off only when the OOB Logoff feature has been enabled through the CAM web console.

Note If **Popup Login Window** is disabled on the taskbar menu, the user can always right-click the Agent icon from the system tray and select **Login** to bring up the login dialog.

Windows 8 Metro and Metro App Support —Toast Notifications

In NAC Agent scenarios where the user does not get network access, like “Remediation Failed” or “Network Access expired”, the Agent displays the following message:

Network not available, Click "OK" to continue" toast notification

To get more details, you can select the toast and you will be redirected to Desktop mode and the NAC agent dialog is displayed.

Toast Notification is displayed for all positive recommended actions that the user needs to perform to gain network access. The following are some examples:

- For Network Acceptance policy, toast will be displayed as: *“Click **Accept** to gain network access”*
- For Agent/Compliance Module Upgrade, toast will be displayed as: *“Click **OK** to Upgrade/Update”*
- In the “user logged out” event, when “Auto Close” option for Logoff is not enabled in CAM, toast notification is provided. This toast enables the users to know that they have been logged out and that they need to login again to get network access.

Auto-Upgrade for Already-Installed Agents: When the Cisco NAC Agent is already installed, users are prompted to auto-upgrade at each login, unless you disable upgrade notification. You can optionally force logout at machine shutdown (default is for users to remain logged in at machine shutdown). You can configure auto-upgrade to be mandatory or optional. With mandatory auto-upgrade and a newer version of the Agent available from the CAM, existing Agent users will see the an auto-upgrade prompt at login.

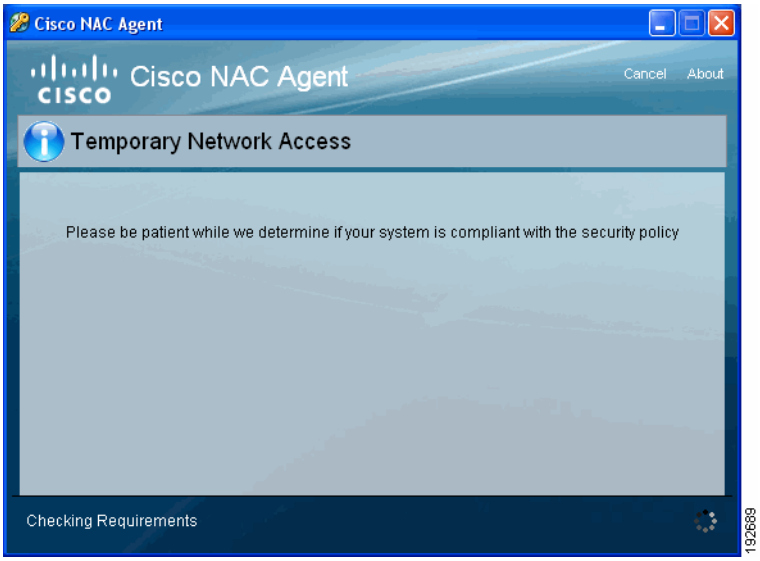
If the upgrade is optional and a newer version of the is Agent available from the CAM, users can choose to **Cancel** the upgrade and continue with the login process.

Clicking **OK** in either of the above dialogs brings up the setup wizard to upgrade the Cisco NAC Agent to the newest version (Figure 10-8). After Agent upgrade and user login, requirement checking proceeds.

If the Compliance Module feature has been enabled, the users see a prompt to install the NAC Agent Compliance Module. If you click **OK**, a setup wizard appears to upgrade the Cisco NAC Agent to the newest version of NAC Agent Compliance Module.

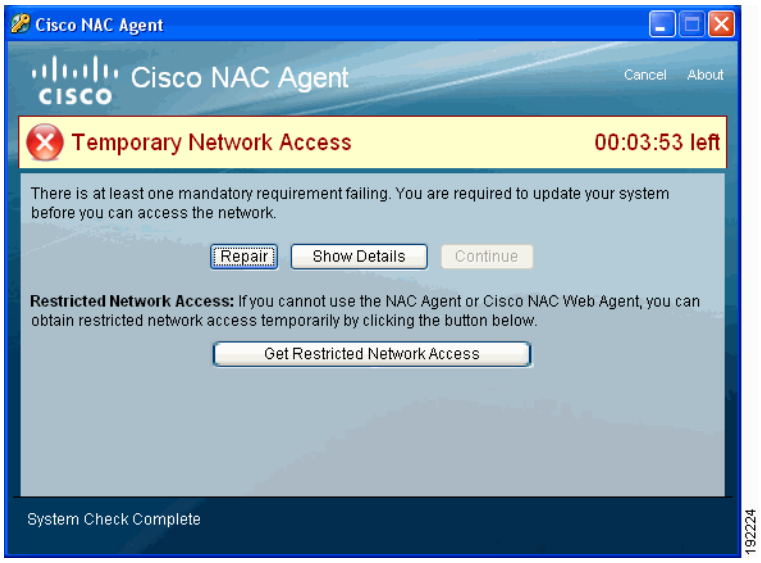
15. After the user submits his or her credentials, the Cisco NAC Agent automatically checks whether the client system meets the requirements configured for the user role (Figure 10-17).

Figure 10-17 Cisco NAC Agent Verifying System



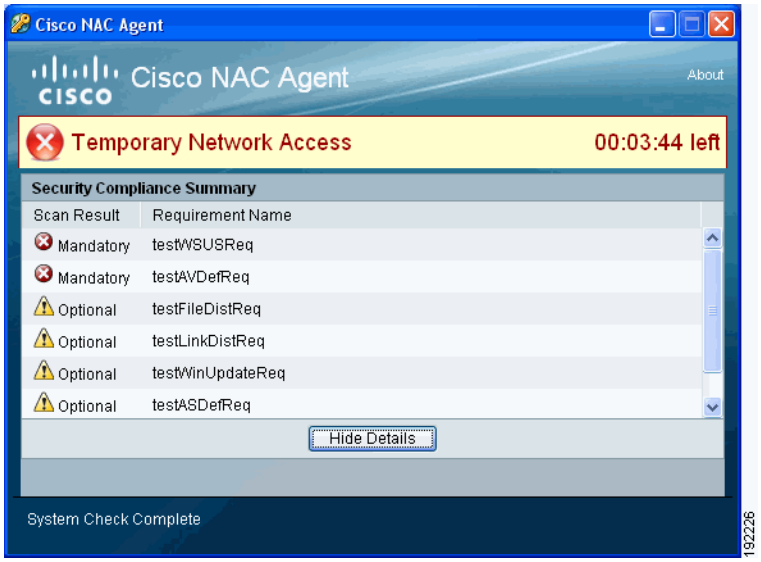
16. If required software is determined to be missing, the **Temporary Network Access** dialog appears (Figure 10-18). The user is assigned to the Agent Temporary role for the session timeout indicated in the dialog. The Temporary role session timeout is set by default to 4 minutes and should be configured to allow enough time for users to access web resources and download the installation package for the required software.

Figure 10-18 Temporary Access—Requirement Not Met


Cisco NAC Agent
Cisco NAC Agent
Cancel
About
Temporary Network Access
00:03:53 left
There is at least one mandatory requirement failing. You are required to update your system before you can access the network.
Repair
Show Details
Continue
Restricted Network Access: If you cannot use the NAC Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
System Check Complete
192224

If the user clicks **Show Details**, the Cisco NAC Agent displays a list of the requirements the user must resolve before Cisco NAC Appliance grants the client machine network access based on the user's assigned role (Figure 10-19).

Figure 10-19 Temporary Network Access—Show Details

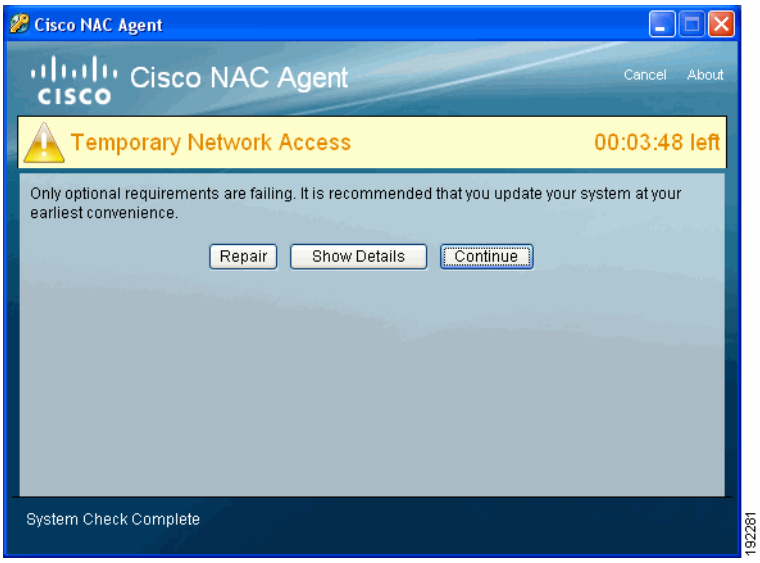


To close the Security Compliance Summary dialog, click **Hide Details**.

17. When the user clicks **Repair**, the Cisco NAC Agent dialog for the requirement with the highest priority configured for the user role appears prompting the user to take appropriate action to address the requirement type.

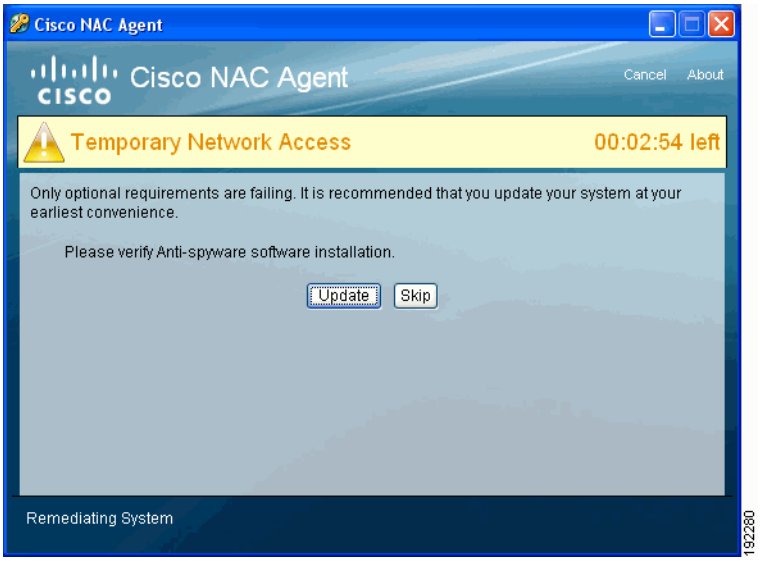
    For an **AV Definition Update** requirement (Figure 10-20), the user clicks the **Update** button to update the client AV software on the system.

Figure 10-20 AV Definition Update Requirement Example



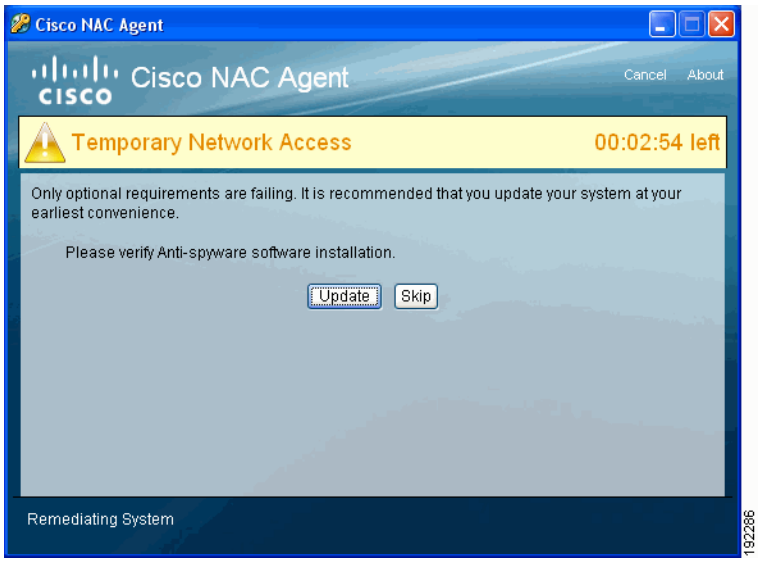
For an **AS Definition Update** requirement (Figure 10-21), the user clicks the **Update** button to update the definition files for the Anti-Spyware software on the client system.

Figure 10-21 AS Definition Update Requirement Example



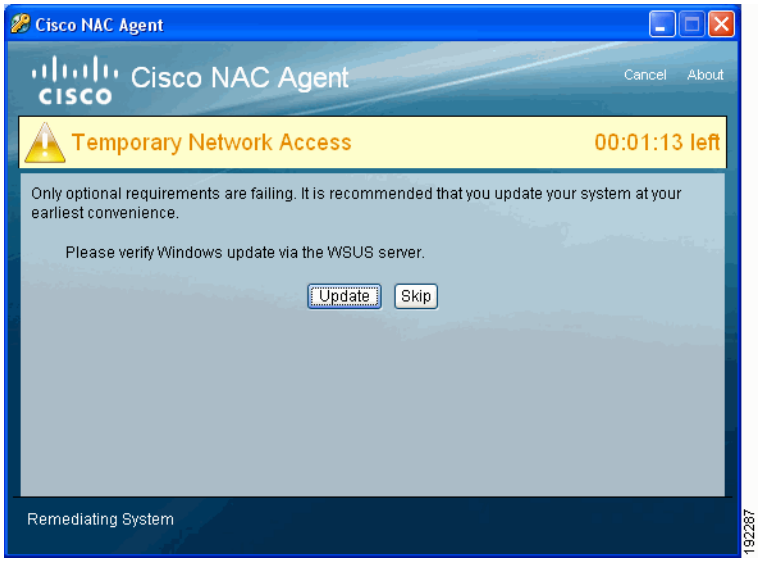
For a **Windows Update** requirement (Figure 10-22), the user clicks the **Update** button to set the Windows Update and force updates on the client system if "Automatically Download and Install" is configured for the requirement.

Figure 10-22 Windows Update Requirement Example



For a **Windows Server Update Service** requirement (Figure 10-23), the user clicks the **Update** button to set the Windows Server Update Service and force updates on the client system.

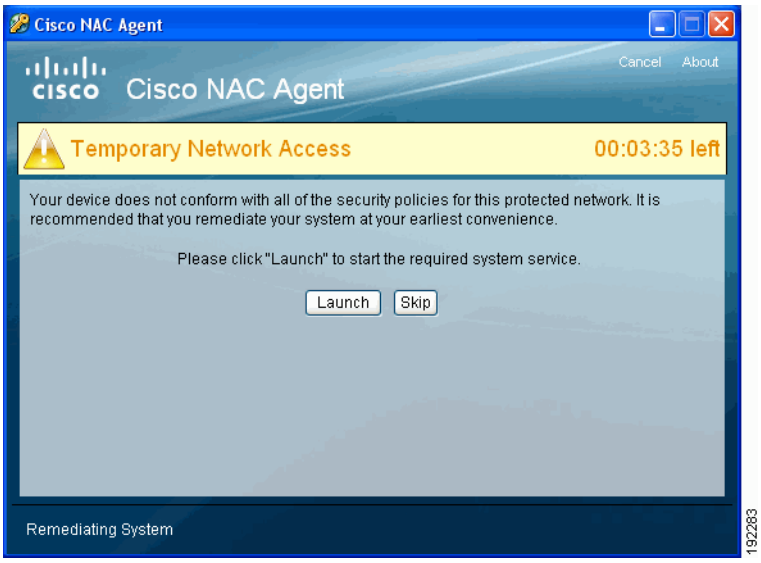
Figure 10-23 Windows Server Update Service Requirement Example



For a **Launch Program** requirement (Figure 10-24), the user clicks the **Launch** button to automatically launch the qualified program for remediation if the requirement is not met.

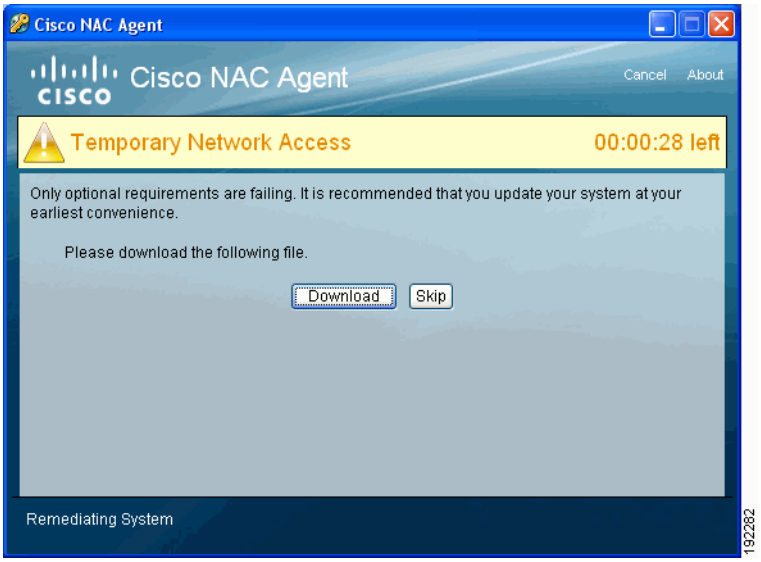
Note Signature processing is governed based on the setting in the config file for Admin, <SignatureCheck>0|1</SignatureCheck>. Signature verification is done regardless of the setting in the config file for non-Admin.

Figure 10-24 Launch Program Requirement Example


Cisco NAC Agent
Cisco NAC Agent
Cancel
About
Temporary Network Access
00:03:35 left
Your device does not conform with all of the security policies for this protected network. It is recommended that you remediate your system at your earliest convenience.
Please click "Launch" to start the required system service.
Launch
Skip
Remediating System
192283

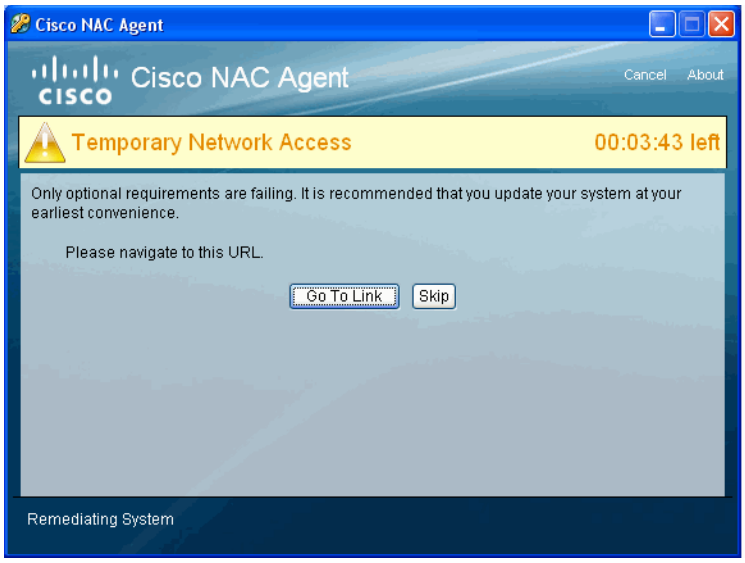
For a **File Distribution** requirement (Figure 10-25), the button displays **Download** instead of **Go To Link**. When the user clicks download, the **Save file to** dialog appears. The user needs to save the installation file to a local folder, and run the executable file from there. (The maximum file size you can make available to users via **File Distribution** is 500MB.)

Figure 10-25 File Distribution Requirement Example



For a **Link Distribution** requirement (Figure 10-26), the user can access the website for the required software installation file by clicking **Go To Link**. This opens a browser for the URL specified in the Location field.

Figure 10-26 Link Distribution Requirement Example

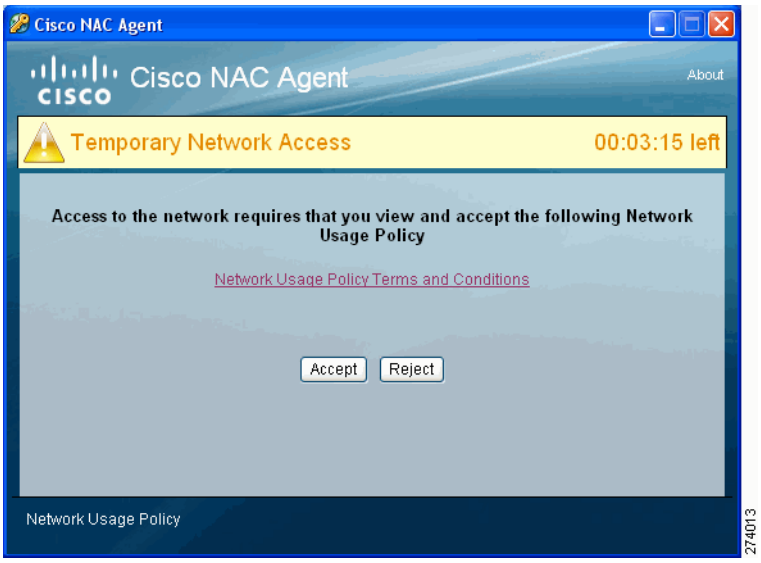


18. Clicking **Cancel** at this stage stops the login process.
19. For each requirement, the user needs to click **Skip** to proceed after completing the action required (Update, Go To Link, Download). The Cisco NAC Agent again performs a scan of the system to verify that the requirement is met. If met, the Agent proceeds to the next requirement configured for the role.

Note If a requirement is **Optional**, when the user clicks **Skip** in the Cisco NAC Agent for the optional requirement, the next requirement dialog appears or the login success dialog appears (Figure 10-28) if all other requirements are met.

20. If a Network Policy page was configured for the role, the following dialog will appear (Figure 10-27) after requirements are met. The user can view the "network usage policy" HTML page (uploaded to the CAM or external server) by clicking the **Network Usage Terms & Conditions** link. The user must click the **Accept** button to successfully log in.

Figure 10-27 Network Policy Dialog

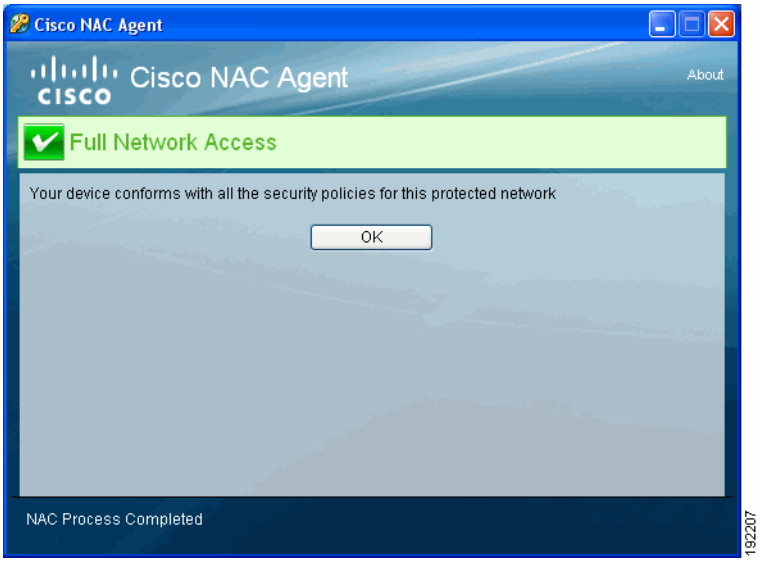


See Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 9-11 for details on configuring this dialog.

21. When all requirements are met (and Network Policy accepted, if configured), the user is transferred from the Temporary role to the normal login role and the login success dialog appears (Figure 10-28). The user is free to access the network as allowed for the normal login role.

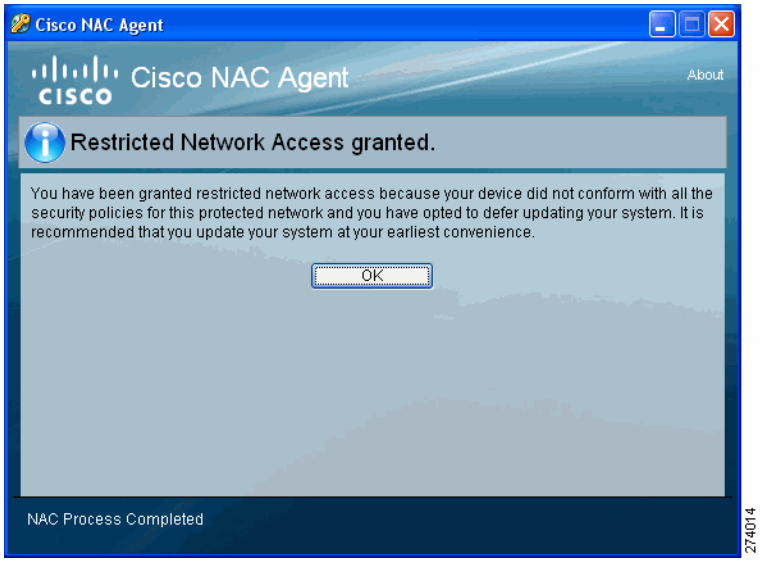
Note The administrator can configure the Login and Logout success dialogs to close automatically after a specified number of seconds, or not to appear at all. See Agent Login, page 1-7 for details.

Figure 10-28 Successful Login—Client Machine Compliant



22. If you have enabled the **Allow restricted network access in case user cannot use Cisco NAC Agent or Cisco NAC Web Agent**" option under **Device Management > Clean Access > General Setup > Agent Login**, or the Agent is currently failing a mandatory requirement, the **Get Restricted Network Access** button appears in the Cisco NAC Agent authentication dialogs and the user can choose to accept restricted network access. Once the user clicks the **Get Restricted Network Access** button, they log into the Cisco NAC Appliance system using a "restricted" user role instead of a more generous standard network access role and are presented with a login confirmation dialog like the one in Figure 10-29. For more information on enabling restricted network access, see Agent Login, page 1-7.

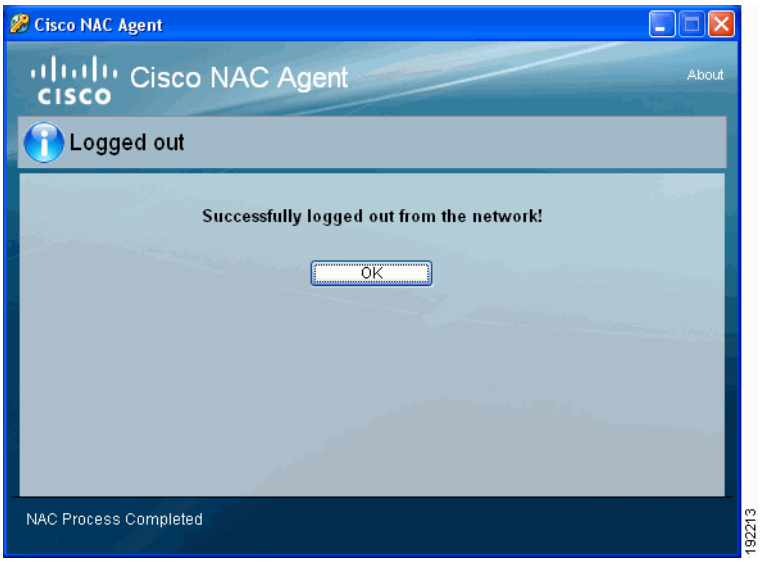
Figure 10-29 Restricted Network Access


Cisco NAC Agent
Cisco NAC Agent
About
Restricted Network Access granted.
You have been granted restricted network access because your device did not conform with all the security policies for this protected network and you have opted to defer updating your system. It is recommended that you update your system at your earliest convenience.
OK
NAC Process Completed
274014

23. To log off the network, the user can right-click the Cisco NAC Agent icon in the system tray and select **Logout**. The logout screen appears (Figure 10-30). If the administrator removes the user from the network, the **Login** dialog will reappear instead (if **Popup Login Window** is set).

Note The administrator can configure the Login and Logout success dialogs to close automatically after a specified number of seconds, or not to appear at all. See Agent Login, page 1-7 for details.

Figure 10-30 Successful Logout



24. Once a user has met requirements, the user will pass these Cisco NAC Agent checks at the next login unless there are changes to the user's computer or Cisco NAC Agent requirements.
25. If a required software installation requires users to restart their computers, the user should log out of the network before restarting. Otherwise, the user is still considered to be in the Temporary role until the session times out. The session timeout and heartbeat check can be set to disconnect users who fail to logout of the network manually.

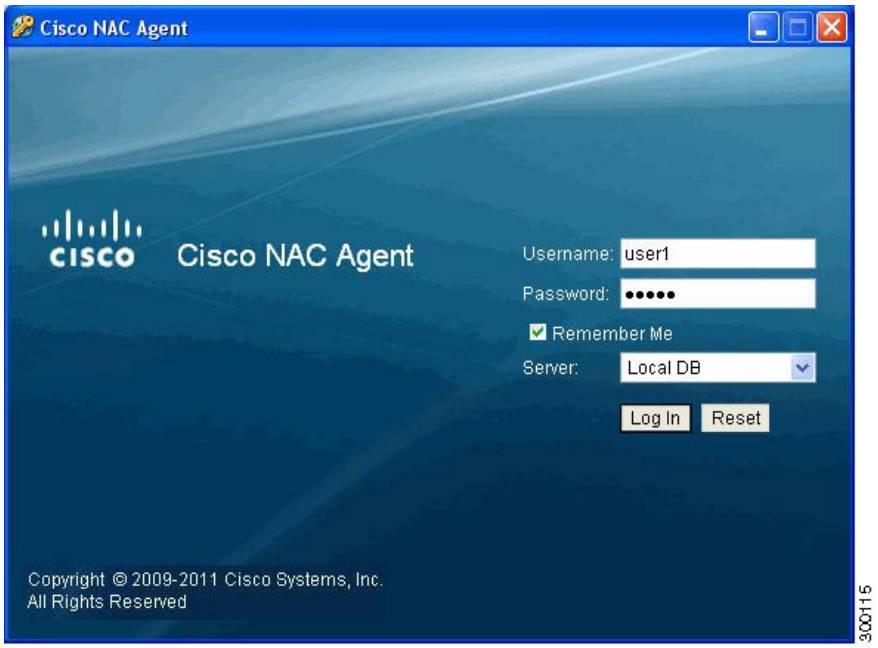
RADIUS Challenge-Response Cisco NAC Agent Dialogs

If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the end-user Cisco NAC Agent login session may feature extra authentication challenge-response dialogs not available in other dialog sessions—beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session.

The following section provides and example of the dialog exchange for Windows Cisco NAC Agent user authentication.

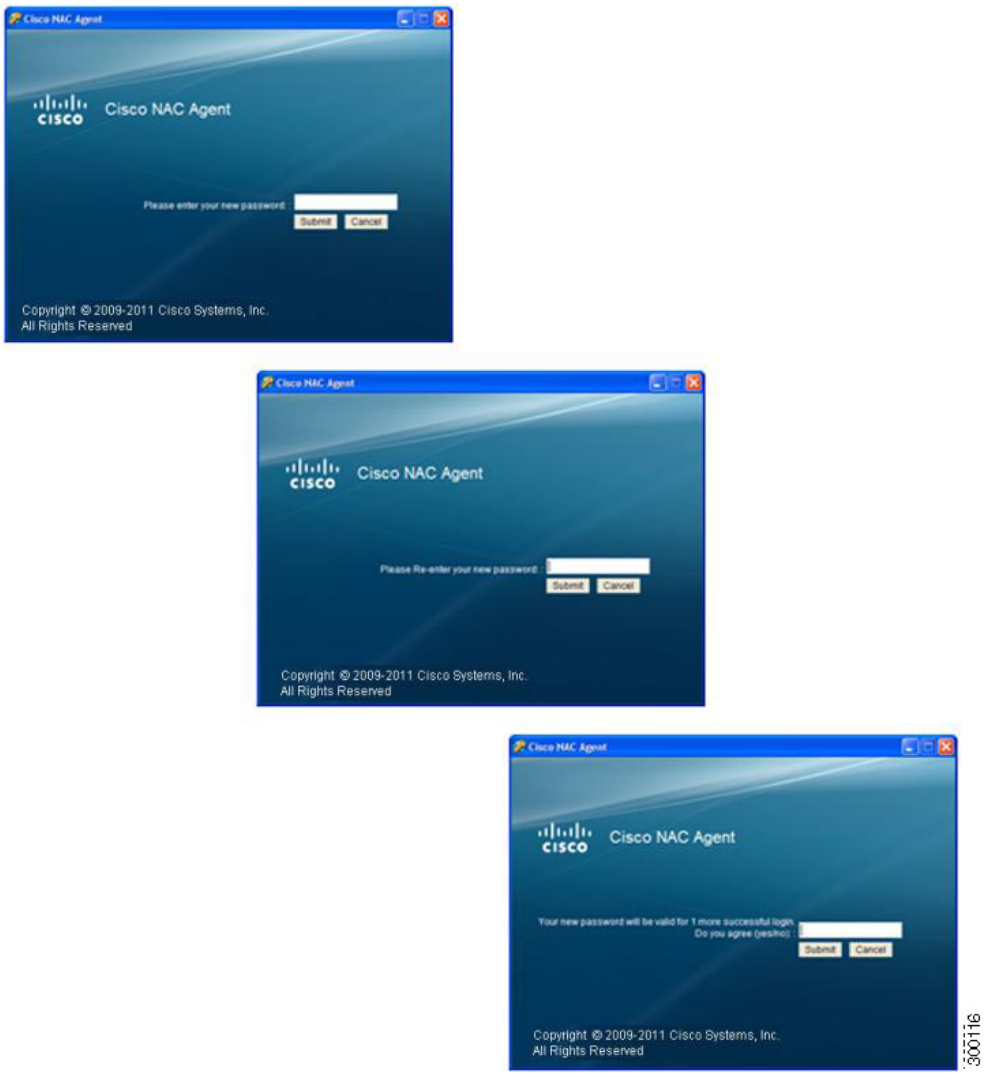
1. The remote user logs in normally and provides their username and password as shown in Figure 10-31.

Figure 10-31 Windows Agent Login Dialog



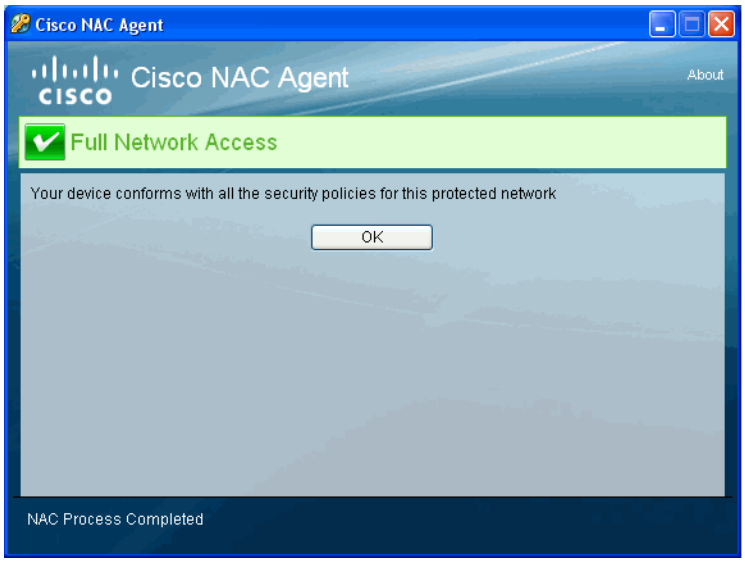
2. If the associated RADIUS server has been configured to authenticate users with additional credentials, the user is presented with one or more additional challenge-response dialogs (like the password renewal scenario shown in Figure 10-32) for which they must provide additional credentials to authenticate and connect.

Figure 10-32 Additional Windows RADIUS Challenge-Response Session Dialog



3. Once the additional challenge-response(s) are validated, the RADIUS server notifies the Clean Access Manager that the user has successfully authenticated and should be granted remote access.

Figure 10-33 Windows RADIUS Challenge-Response Authentication Successful



Cisco NAC Web Agent

This chapter describes how to configure the Cisco NAC Web Agent to allow users to log in to the network without requiring a permanent, dedicated network access application on the client machine.

- Overview, page 10-25
- Configuration Steps for the Cisco NAC Web Agent, page 10-27
- Cisco NAC Web Agent User Dialogs, page 10-28

Overview

Warning **Cisco does not recommend using the Cisco NAC Web Agent on client machines connecting with link speeds slower than 56Kbits/s.**

The Cisco NAC Web Agent provides temporal posture assessment for client machines. Users launch the Cisco NAC Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet. When the user terminates the Web Agent session, the Web Agent logs the user off of the network and their user ID disappears from the Online Users list.

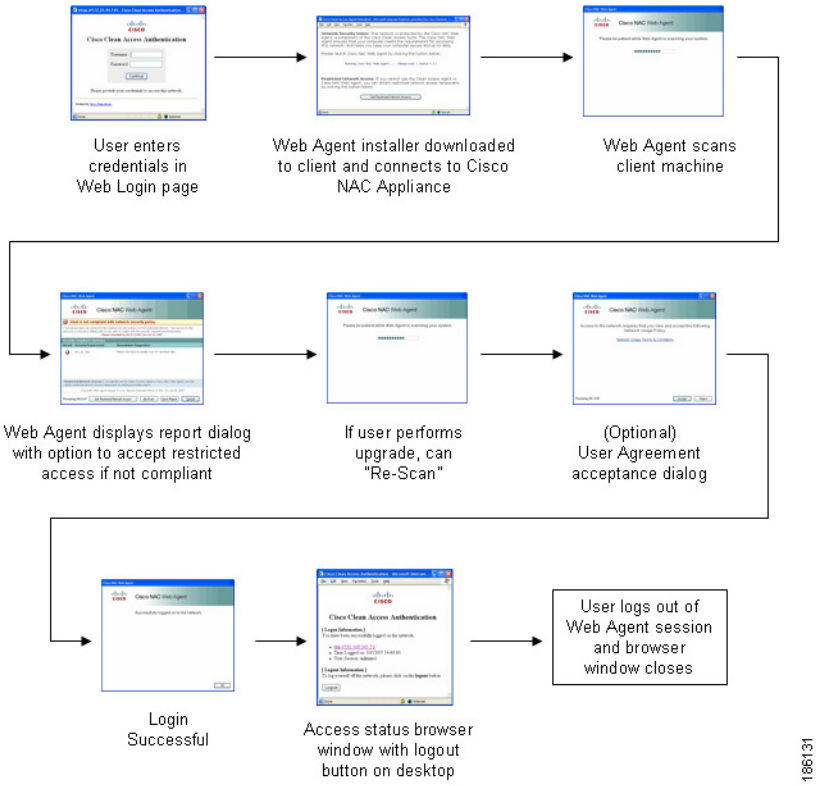
After users log into the Cisco NAC Web Agent, the Web Agent gets the requirements configured for the user role/OS from the Clean Access Server, checks the host registry, processes, applications, and services for required packages and sends a report back to the CAM (via the CAS). If requirements are met on the client, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each unmet requirement. The dialog (configured in the New Requirement form) provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept "restricted" network access (if you have enabled that option in the **Device Management > Clean Access > General Setup > Agent Login** page) while they try to remediate the client machine so that it meets

requirements for the user login role. You can set up a “restricted” user role to provide access to only limited applications/network resources in the same way you configure a standard user login role according to the guidelines in Adding a New User Role, page 6-7.

Cisco NAC Web Agent posture assessment is configured in the CAM by creating requirements based on rules and (optionally) checks, then applying the requirements to user roles/client operating systems. This chapter describes how to configure these requirements.

Figure 10-34 illustrates the general user sequence for launching the Cisco NAC Web Agent, if the administrator has required use of the Cisco NAC Web Agent for the user’s role and operating system.

Figure 10-34 Cisco NAC Web Agent User Interaction/Experience


User enters credentials in Web Login page
Web Agent installer downloaded to client and connects to Cisco NAC Appliance
Web Agent scans client machine
Web Agent displays report dialog with option to accept restricted access if not compliant
If user performs upgrade, can "Re-Scan"
(Optional) User Agreement acceptance dialog
Login Successful
Access status browser window with logout button on desktop
User logs out of Web Agent session and browser window closes
186131

System Requirements

Your Cisco NAC Appliance network must meet the following requirements to support the Cisco NAC Web Agent:

- Operating System Compatibility and Browser Support
- ActiveX and Java Applet Requirements
- Microsoft Internet Explorer 7 in Windows Vista

Operating System Compatibility and Browser Support

If users are logging in via the Web Agent in a Windows 7 environment and have proxy connections configured on Internet Explorer, they must enable “Protected Mode” in the browser’s security settings to enable Web Agent download on the client machine.

You can find complete Operating System Compatibility and Browser Support information for all Cisco NAC Appliance Agents in the *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.

In Windows 8, Web Agent does not support Metro Mode and Toast Notification.

ActiveX and Java Applet Requirements

- If you plan to use the Java applet version to install the Web Agent files, the client must already have Java version 1.5 or higher installed.
- If you plan to install the Web Agent files via ActiveX, the client machine must be using 32-bit version of Microsoft Internet Explorer. You cannot install via ActiveX on a Firefox web browser or on a 64-bit verison of Internet Explorer.
- The user must have permissions for ActiveX download or admin privileges on the client machine to enable installation of ActiveX controls.

Note The Web Agent Java applet might fail to launch when the CPU load on the client machine approaches 100%. (ActiveX runs successfully under these conditions.)

Note Security restrictions for the "Guest" user profile in Windows Vista operating systems prevent ActiveX controls and Java applets from running properly. Therefore, you must be logged into the Windows Vista client machine as a known user (not a "Guest") in order to log into Cisco NAC Appliance via the Web Agent.

Microsoft Internet Explorer 7 in Windows Vista

By default, Windows Vista checks the server certificate revocation list and prevents the Web Agent from launching on the client machine. To disable this functionality:

Step 1 In Internet Explorer 7, navigate to **Menu > Tools > Internet Options**.

Step 2 Click the **Advanced** tab.

Step 3 Under Security, uncheck (disable) the **Check for server certificate revocation** option.

Step 4 Click **OK**.

Configuration Steps for the Cisco NAC Web Agent

The basic steps needed to configure the Cisco NAC Appliance system to enable and use the Cisco NAC Web Agent are as follows:

1. Make sure to follow the steps in Agent Configuration Steps, page 9-3 to enable and specify installer download parameters for the Cisco NAC Web Agent.
2. (Optional) Set up a "Restricted Access" role as described in Adding a New User Role, page 6-7.
3. Configure Agent requirements using the instructions in Configuring Agent-Based Posture Assessment, page 9-39:
   a. Configuring AV/AS Definition Update Requirements, page 9-41

b. Configuring a Windows Server Update Services Requirement, page 9-57
c. Configuring a Windows Update Requirement, page 9-64
d. Configuring Custom Checks, Rules, and Requirements, page 9-70
e. Configuring a Launch Programs Requirement, page 9-85
f. Map Requirements to Rules, page 9-90
g. Apply Requirements to User Roles, page 9-92
h. Validate Requirements, page 9-93
i. Configuring an Optional/Audit Requirement, page 9-94

After you have accounted for the above topics, users can log in and gain network access via the Cisco NAC Appliance system according to the parameters and requirements you have defined in your system configuration.

Cisco NAC Web Agent User Dialogs

This section illustrates the user experience when users access your network via the Cisco NAC Web Agent.

Note Depending on the user's privilege level (Administrator, Privileged User, User, etc.) and web browser security settings on the client machine, the user may or may not see additional security "warnings" or message dialogs during critical points in the download and installation process. (For example, the user may need to acknowledge the installation process redirecting the user to a particular URL destination or approve the Web Agent executable launch following client scanning.)

1. When the user first opens a web browser, the user is redirected to the web login page (Figure 10-35).

Figure 10-35 Login Page



2. The user enters their credentials in the web login page and is redirected to the Cisco NAC Web Agent Launch page (Figure 10-36) where they can choose to launch the Cisco NAC Web Agent ActiveX or Java Applet installer. You determine the installer launch method using the **Web Client (ActiveX/Applet)** option in the **Administration > User Pages > Login Page** configuration screen.

Note If you plan to install the Web Agent files via ActiveX, the client machine must be using 32-bit version Microsoft Internet Explorer. You cannot install via ActiveX on a Firefox web browser or on a 64-bit version of Internet Explorer.

Figure 10-36 Cisco NAC Web Agent Launch Page

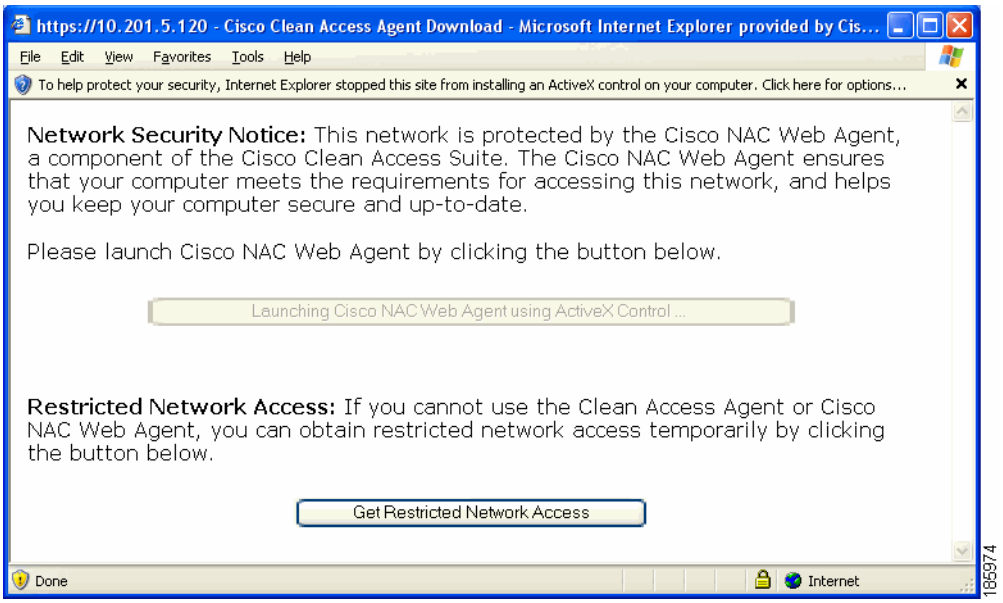

Cisco NAC Web Agent Download
Page
Safety
Tools
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco NAC Appliance Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please launch Cisco NAC Web Agent by clicking the button below.
Launch Cisco Web Agent 4.9.5.3
Network Security Notice: This network is protected by a Cisco NAC Appliance Agent, a component of the Cisco NAC Appliance Suite. The Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please use the Agent to log in to the network.
If you don't have the Agent software yet, download it by clicking the button below. After downloading the installation file, run it to complete the installation.

3. The user clicks the **Launch Cisco NAC Web Agent** button (the button will display the version of the Web Agent being installed).

Note If the "**Allow restricted network access in case user cannot use Cisco NAC Web Agent**" option is selected under **Device Management > Clean Access > General Setup > Agent Login**, the **Get Restricted Network Access** button and related text will display in the Download Cisco NAC Web Agent page. See Agent Login, page 1-7 for details.

Note If the existing CAS certificate is not trusted on the client, the user must accept the optional certificate in the **Security Alert** dialog that appears before Web Agent launch can successfully proceed.

Figure 10-37 ActiveX Installation Notice


https://10.201.5.120 - Cisco Clean Access Agent Download - Microsoft Internet Explorer provided by Cis...
File Edit View Favorites Tools Help
To help protect your security, Internet Explorer stopped this site from installing an ActiveX control on your computer. Click here for options...
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco Clean Access Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please launch Cisco NAC Web Agent by clicking the button below.
Launching Cisco NAC Web Agent using ActiveX Control ...
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Done
Internet
185974

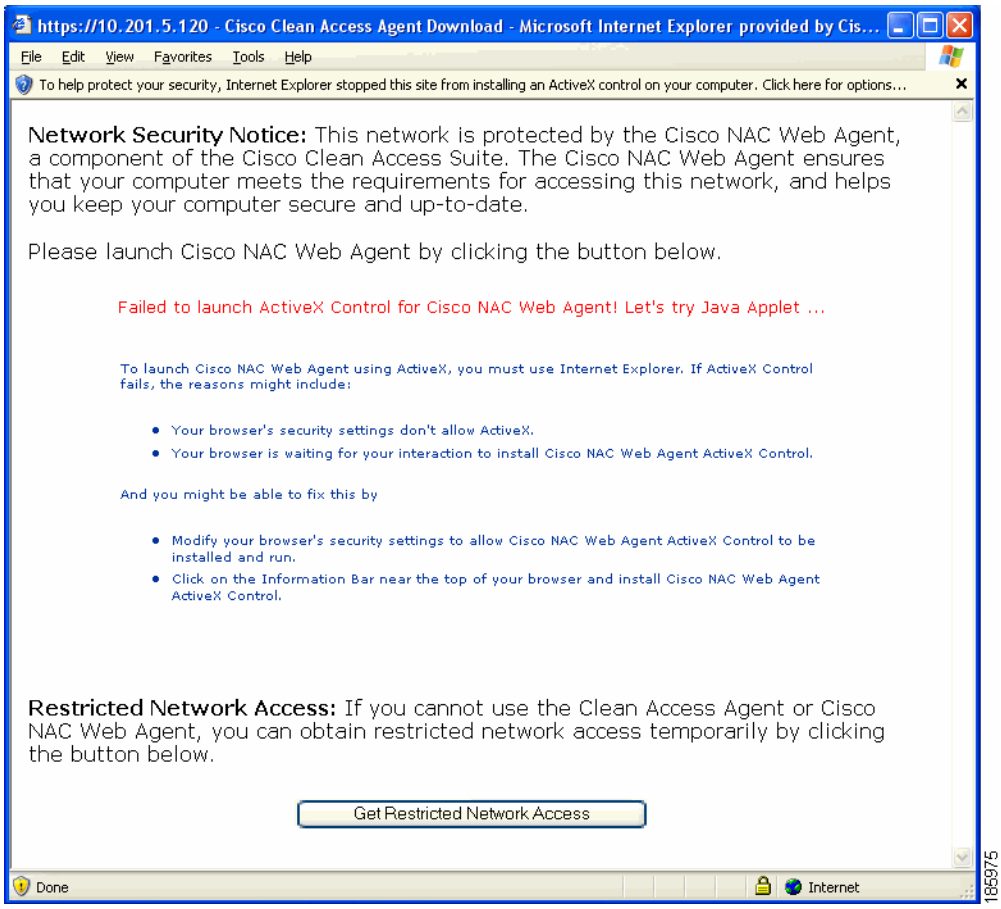
4. If the user's web browser settings are configured to verify actions like installing an ActiveX control on the client machine, the user may need to verify the action. For example, in the case of Microsoft IE, the user may need to click on a status bar that appears in the browser window and choose the **Install ActiveX Control** option from the resulting pop-up to validate the ActiveX process.

   If the ActiveX control fails to initialize, the user sees an ActiveX installation notice like the one in Figure 10-38 and if you have set up the Cisco NAC Appliance system to try to download the Web Agent install files via Java applet should the ActiveX method fail, the Cisco NAC Appliance system attempts to download the Web Agent installation files via Java applet.

   Otherwise, the user will not be able to use the Cisco NAC Web Agent for login and will either have to contact the Cisco NAC Appliance network administrator to try and help troubleshoot issues with the installation process, or accept "Restricted" network access for the time being until they can fix the Web Agent installation problem.

Note If you specify that the Java applet method is preferred using the **Web Client (ActiveX/Applet)** option in the **Administration > User Pages > Login Page** configuration screen, the order of these possibilities is reversed—the user sees a Java applet failure notice before the ActiveX control attempts to install the Web Agent files on the client machine.

Figure 10-38 ActiveX Installation Notice


https://10.201.5.120 - Cisco Clean Access Agent Download - Microsoft Internet Explorer provided by Cis...
File Edit View Favorites Tools Help
To help protect your security, Internet Explorer stopped this site from installing an ActiveX control on your computer. Click here for options...
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco Clean Access Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please launch Cisco NAC Web Agent by clicking the button below.
Failed to launch ActiveX Control for Cisco NAC Web Agent! Let's try Java Applet ...
To launch Cisco NAC Web Agent using ActiveX, you must use Internet Explorer. If ActiveX Control fails, the reasons might include:
Your browser's security settings don't allow ActiveX.
Your browser is waiting for your interaction to install Cisco NAC Web Agent ActiveX Control.
And you might be able to fix this by
Modify your browser's security settings to allow Cisco NAC Web Agent ActiveX Control to be installed and run.
Click on the Information Bar near the top of your browser and install Cisco NAC Web Agent ActiveX Control.
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Done
Internet
185975

Note If the version of the Agent being downloaded from the CAM is "unsigned" (if it has been handed over directly from Cisco Support as a patch version, for example), the user may see an additional Java Security Notice like the one in Figure 10-39.

Figure 10-39 Java Applet Security Notice


Warning - Security
Do you want to accept the certificate from web site "10.201.5.120" for the purpose of exchanging encrypted information?
Publisher authenticity verified by: "Perfigo, Inc."
The security certificate was issued by a company that is not trusted.
The security certificate has not expired and is still valid.
Caution: "10.201.5.120" asserts that this content is safe. You should only accept this content if you trust "10.201.5.120" to make that assertion.
More Details
Yes
No
Always
185979

If both the ActiveX and Java applet Web Agent download and install methods fail, the user sees a notification screen like the one in Figure 10-40 and is presented with a Windows dialog informing the user that Cisco NAC Web Agent login failed (Figure 10-41).

Note For more information on status and error codes the ActiveX Control or Java Applet passes back to the Cisco NAC Appliance system, see Table 11-4 in Cisco NAC Web Agent Status Codes, page 11-40.

Figure 10-40 ActiveX and Java Installation Failure Notice

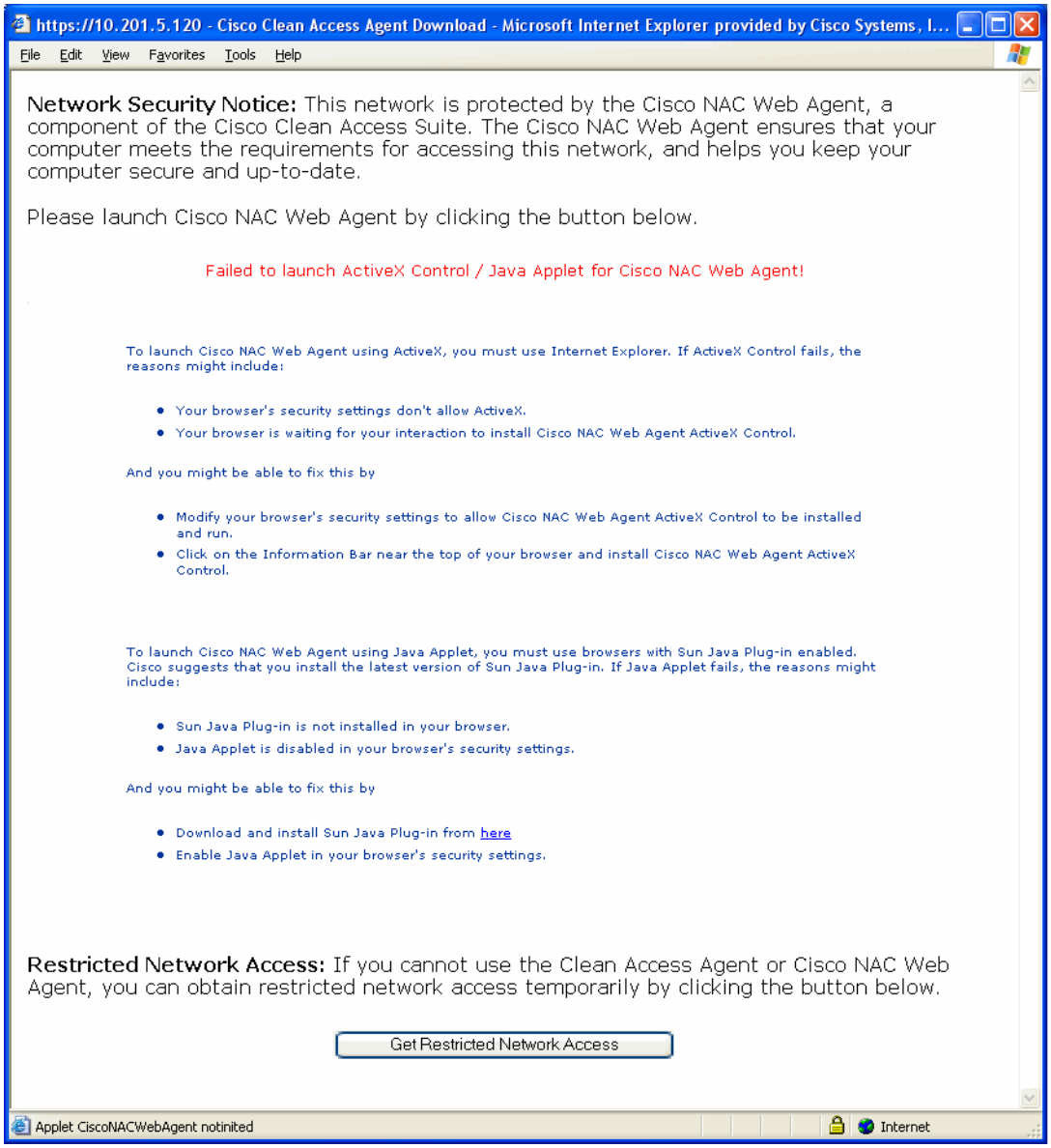
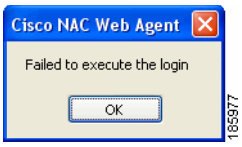
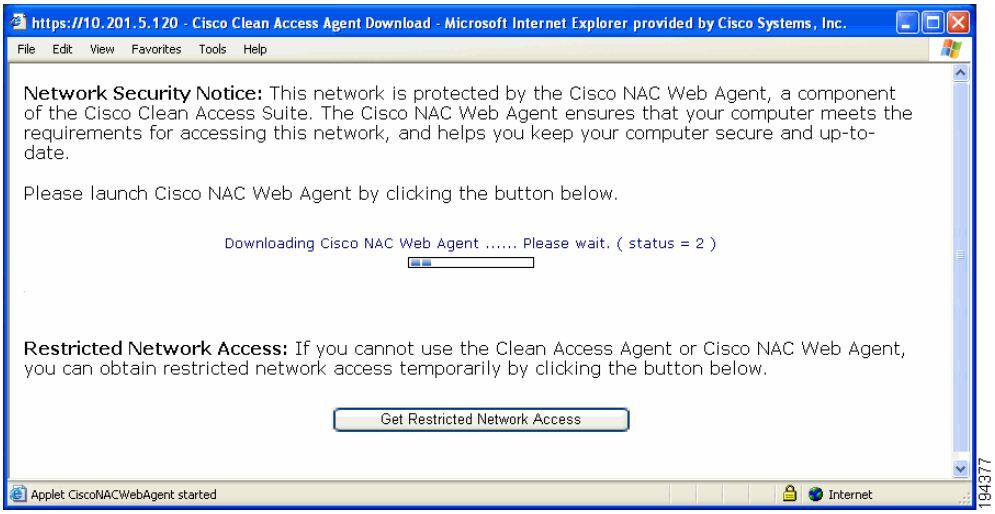

https://10.201.5.120 - Cisco Clean Access Agent Download - Microsoft Internet Explorer provided by Cisco Systems, I...
File Edit View Favorites Tools Help
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco Clean Access Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please launch Cisco NAC Web Agent by clicking the button below.
Failed to launch ActiveX Control / Java Applet for Cisco NAC Web Agent!
To launch Cisco NAC Web Agent using ActiveX, you must use Internet Explorer. If ActiveX Control fails, the reasons might include:
Your browser's security settings don't allow ActiveX.
Your browser is waiting for your interaction to install Cisco NAC Web Agent ActiveX Control.
And you might be able to fix this by
Modify your browser's security settings to allow Cisco NAC Web Agent ActiveX Control to be installed and run.
Click on the Information Bar near the top of your browser and install Cisco NAC Web Agent ActiveX Control.
To launch Cisco NAC Web Agent using Java Applet, you must use browsers with Sun Java Plug-in enabled. Cisco suggests that you install the latest version of Sun Java Plug-in. If Java Applet fails, the reasons might include:
Sun Java Plug-in is not installed in your browser.
Java Applet is disabled in your browser's security settings.
And you might be able to fix this by
Download and install Sun Java Plug-in from here
Enable Java Applet in your browser's security settings.
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Applet CiscoNACWebAgent notinited
Internet
185976

Figure 10-41 Cisco NAC Web Agent Login Failure Notice



5. After the user allows the ActiveX control to install the Web Agent files or acknowledges the Java certificate security warning and chooses to accept the Java applet contents, the Web Agent installer goes to work installing the Web Agent executable and all required ancillary files in a temporary directory con the client machine (like **C:\Temp**, for example) and the browser window displays a "Downloading Cisco NAC Web Agent..." message similar to Figure 10-42.

Figure 10-42 Cisco NAC Web Agent Executable Download

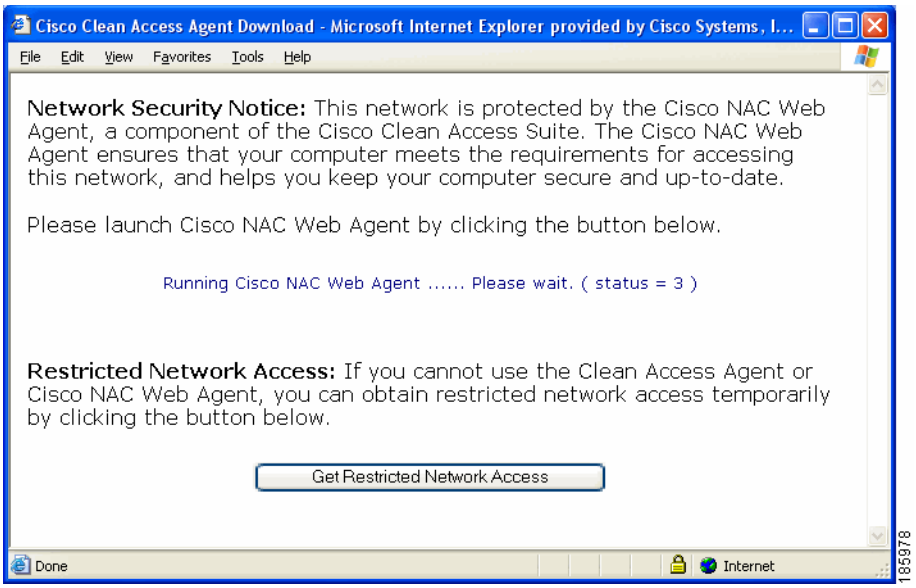

https://10.201.5.120 - Cisco Clean Access Agent Download - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco Clean Access Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please launch Cisco NAC Web Agent by clicking the button below.
Downloading Cisco NAC Web Agent ..... Please wait. (status = 2)
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Applet CiscoNACWebAgent started
Internet
194377

The downloading step in the process can take anywhere from just a few seconds to several minutes, depending on your connection speed. Typically, a fast connection speed like a 10/100 Ethernet LAN link will take very little time, whereas a relatively slow connection link like ISDN could take significantly longer.

Warning **Cisco does not recommend using the Cisco NAC Web Agent on client machines connecting with link speeds slower than 56Kbits/s.**

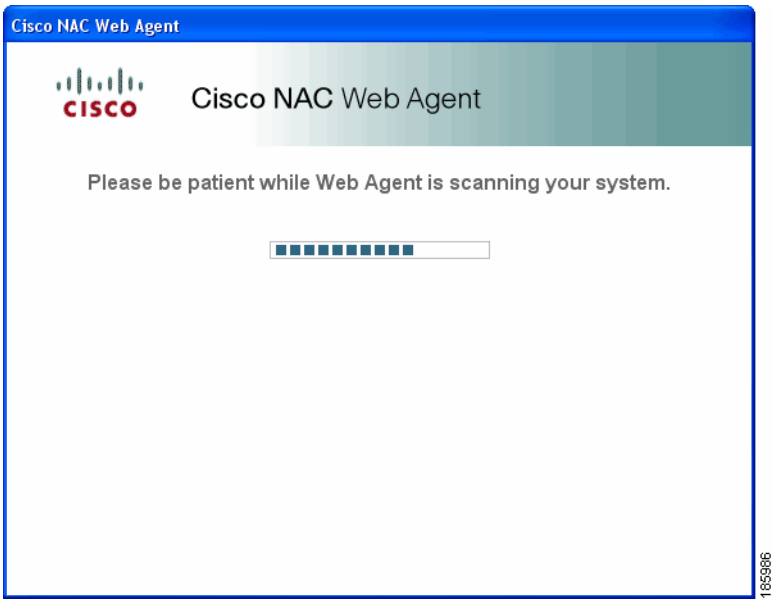
Once the executable files have been downloaded to the client machine's local temporary file directory, the self-extracting installer automatically begins launching the Web Agent on the client machine and the user sees a status window similar to Figure 10-43.

Figure 10-43 Cisco NAC Web Agent Installation


Cisco Clean Access Agent Download - Microsoft Internet Explorer provided by Cisco Systems, I...
File Edit View Favorites Tools Help
Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco Clean Access Suite. The Cisco NAC Web Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date.
Please launch Cisco NAC Web Agent by clicking the button below.
Running Cisco NAC Web Agent ..... Please wait. (status = 3)
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Get Restricted Network Access
Done
Internet
185978

6. When the ActiveX control or Java Applet session completes, the Cisco NAC Web Agent automatically checks whether the client system meets the requirements configured for the user role. (See Figure 10-44.)

Figure 10-44 Cisco NAC Web Agent Scanning Dialog



7. If the Web Agent scan determines that a *required* application, process, or critical update is missing, the user receives a "Host is not compliant with network security policy" message (Figure 10-45 through Figure 10-50 provide a range of examples), is assigned to the Cisco NAC Web Agent Temporary role for the session timeout indicated in the dialog (typically 4 minutes by default).

Note For information on status codes the Cisco NAC Web Agent passes back to the Cisco NAC Appliance system, see Table 11-5 in Cisco NAC Web Agent Status Codes, page 11-40.

8. The user can choose to do one or more of the following:
   - Click **Cancel** to abort Web Agent launch
   - Click **Save Report** to save a local copy of the Web Agent session report that the user can forward on to the Cisco NAC Appliance administrator to help troubleshoot potential Web Agent login issues

     Web Archive, Single File (*.mht)—Limited to the Microsoft Internet Explorer browser only

     Web Page, Complete (*.htm, html)—Supports any browser, but resource files (GIFs, CSS, etc.) are stored in a subdirectory

     Web Page, HTML Only (*htm, *.html)—Format and GIFs will not be present

     Text File (*.txt)

     Note Because the report dialog makes use of IFRAMEs, the report data and restricted access data are stored in a separate HTML file. If the **HTML Only** and **Text** options are used, the user does not see the report and restricted data in the saved file.

   - Click **Get Restricted Network Access** to log into the Cisco NAC Appliance system using a "restricted" user role instead of a more generous standard network access role.
   - Perform manual remediation—the user can download installation packages for the required software and perform other required remediation tasks according to the Remediation Suggestion entries displayed and click **Re-Scan** to see if their changes bring the client machine into acceptable compliance.

Note The Temporary role session timeout is set to 4 minutes by default, but Cisco recommends you configure the duration to allow enough time for users to access web resources, download installation packages for the required software, and possibly perform other required remediation tasks before attempting to **Re-Scan** the client machine for compliance.

Figure 10-45 Mandatory AV Definition Requirement Not Met

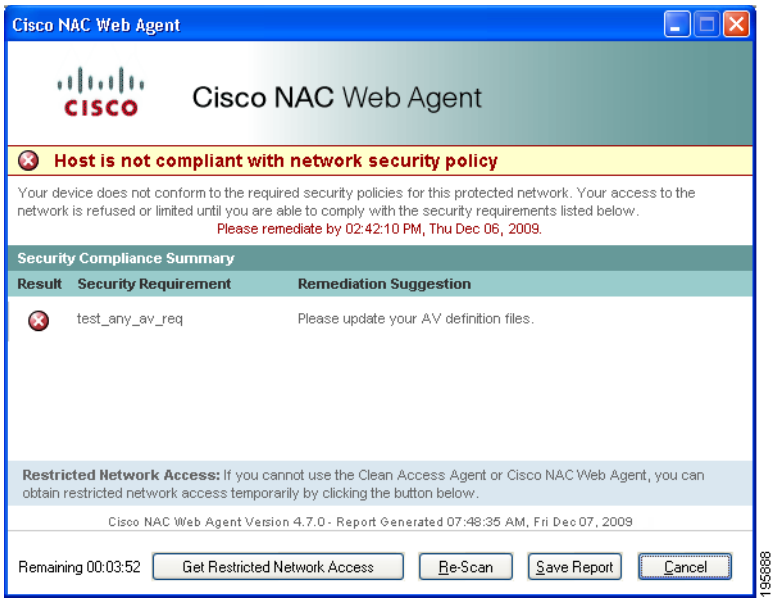

Cisco NAC Web Agent
Cisco NAC Web Agent
Host is not compliant with network security policy
Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 02:42:10 PM, Thu Dec 06, 2009.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
test_any_av_req
Please update your AV definition files.
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:52
Get Restricted Network Access
Re-Scan
Save Report
Cancel
195888

Figure 10-46 Mandatory AS Definition Update Requirement Not Met

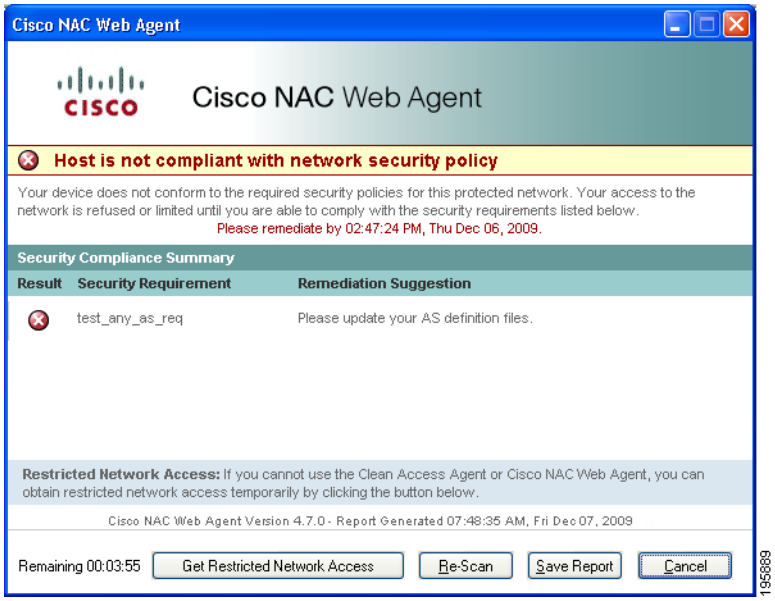

Cisco NAC Web Agent
Cisco NAC Web Agent
Host is not compliant with network security policy
Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 02:47:24 PM, Thu Dec 06, 2009.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
test_any_as_req
Please update your AS definition files.
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:55
Get Restricted Network Access
Re-Scan
Save Report
Cancel
195889

Figure 10-47 Mandatory File Distribution Requirement Not Met

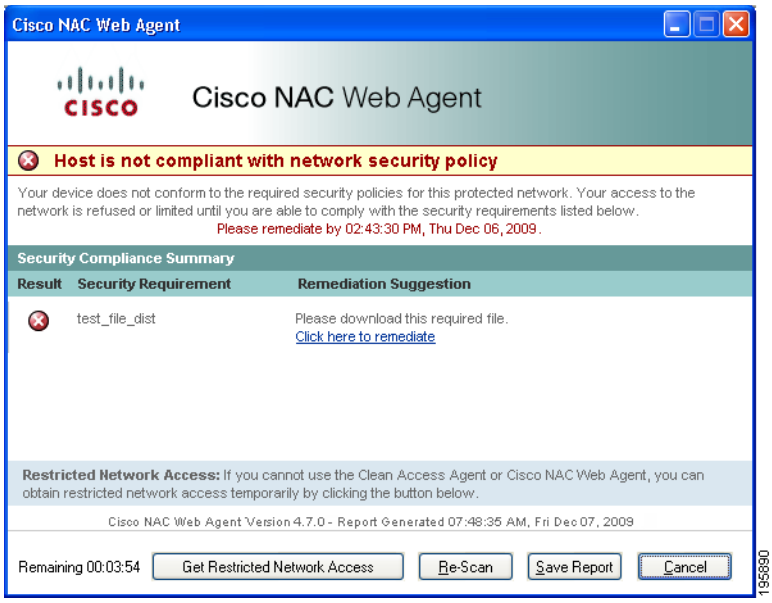

Cisco NAC Web Agent
Cisco NAC Web Agent
Host is not compliant with network security policy
Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 02:43:30 PM, Thu Dec 06, 2009.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
test_file_dist
Please download this required file.
Click here to remediate
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:54
Get Restricted Network Access
Re-Scan
Save Report
Cancel
195890

Figure 10-48 Mandatory Link Distribution Requirement Not Met

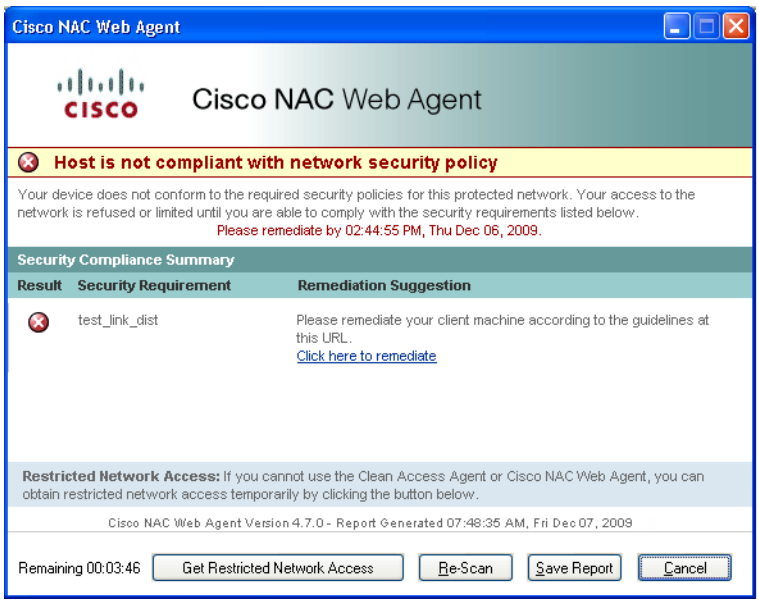

Cisco NAC Web Agent
Cisco NAC Web Agent
Host is not compliant with network security policy
Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 02:44:55 PM, Thu Dec 06, 2009.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
test_link_dist
Please remediate your client machine according to the guidelines at this URL.
Click here to remediate
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:46
Get Restricted Network Access
Re-Scan
Save Report
Cancel
195891

Figure 10-49 Mandatory Local Check Requirement Not Met

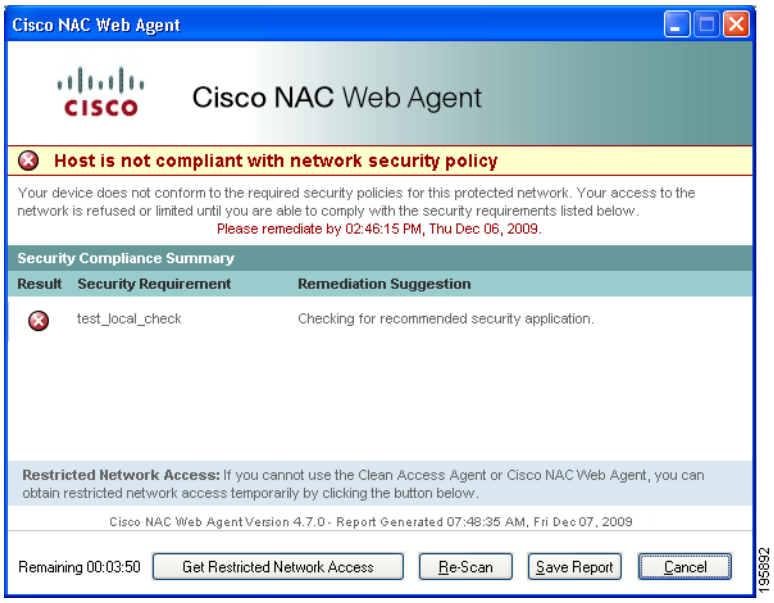
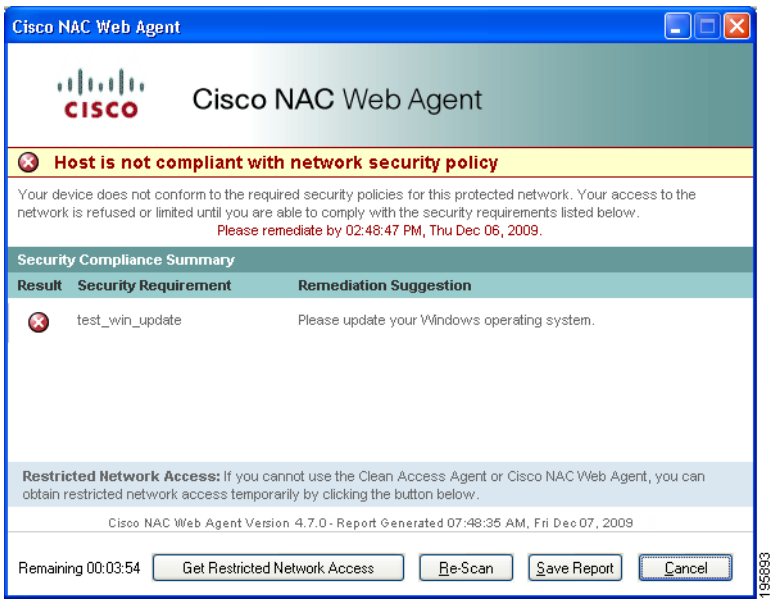

Cisco NAC Web Agent
Cisco NAC Web Agent
Host is not compliant with network security policy
Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 02:46:15 PM, Thu Dec 06, 2009.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
test_local_check
Checking for recommended security application.
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:50
Get Restricted Network Access
Re-Scan
Save Report
Cancel
195892

Figure 10-50 Mandatory Windows Upgrade Requirement Not Met


Cisco NAC Web Agent
Cisco NAC Web Agent
Host is not compliant with network security policy
Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 02:48:47 PM, Thu Dec 06, 2009.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
test_win_update
Please update your Windows operating system.
Restricted Network Access: If you cannot use the Clean Access Agent or Cisco NAC Web Agent, you can obtain restricted network access temporarily by clicking the button below.
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:54
Get Restricted Network Access
Re-Scan
Save Report
Cancel
195893

9. If the Web Agent scan determines that an *optional* application, process, or update is missing, the user receives a "Host is compliant with network security policy" message (Figure 10-51), is assigned to the Cisco NAC Web Agent Temporary role for the session timeout indicated in the dialog (typically 4 minutes by default).

Note For information on status codes the Cisco NAC Web Agent passes back to the Cisco NAC Appliance system, see Table 11-5 in Cisco NAC Web Agent Status Codes, page 11-40.

10. The user can choose to do one the following:
    - Click **Continue** to complete Web Agent launch.
    - Click **Save Report** to save a local copy of the Web Agent session report that the user can forward on to the Cisco NAC Appliance administrator to help troubleshoot potential Web Agent login issues. The reports are available in the following formats:

      Web Archive, Single File (*.mht)—Limited to the Microsoft Internet Explorer browser only

      Web Page, Complete (*.htm, html)—Supports any browser, but resource files (GIFs, CSS, etc.) are stored in a subdirectory

      Web Page, HTML Only (*htm, *.html)—Format and GIFs will not be present

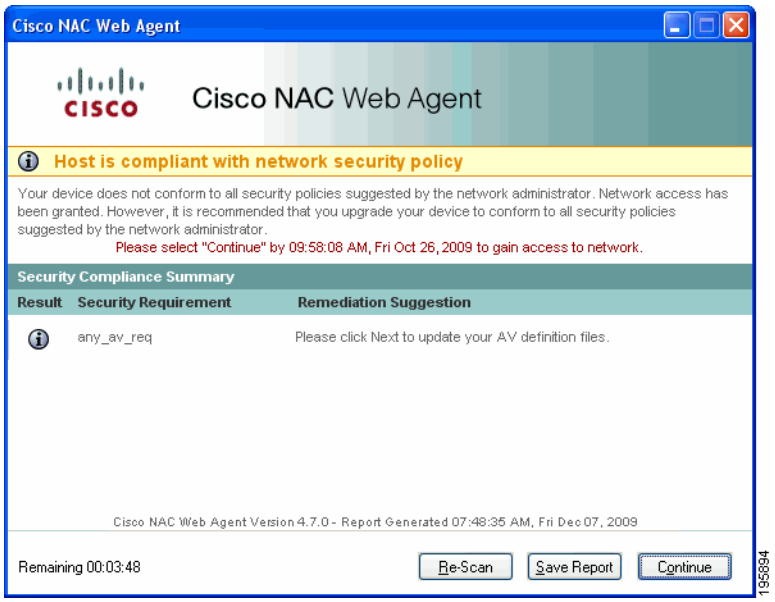
      Text File (*.txt)

      Note Because the report dialog makes use of IFRAMEs, the report data and restricted access data are stored in a separate HTML file. If the **HTML Only** and **Text** options are used, the user does not see the report and restricted data in the saved file.

    - Perform manual remediation—the user can download installation packages for the required software and perform other required remediation tasks according to the Remediation Suggestion entries displayed and click **Re-Scan** to see if their changes bring the client machine into full compliance.

Note The Temporary role session timeout is set to 4 minutes by default, but Cisco recommends you configure the duration to allow enough time for users to access web resources, download installation packages for the required software, and possibly perform other required remediation tasks before attempting to **Re-Scan** the client machine for compliance.

Figure 10-51 Optional Requirement Not Met


Cisco NAC Web Agent
Cisco NAC Web Agent
Host is compliant with network security policy
Your device does not conform to all security policies suggested by the network administrator. Network access has been granted. However, it is recommended that you upgrade your device to conform to all security policies suggested by the network administrator.
Please select "Continue" by 09:58:08 AM, Fri Oct 26, 2009 to gain access to network.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
any_av_req
Please click Next to update your AV definition files.
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:48
Re-Scan
Save Report
Continue
195894

11. If the Web Agent scan determines that the client machine is compliant with the Agent requirements you have configured for the user's role, the user receives a "Host is compliant with network security policy" message within a green banner (Figure 10-52).

Note For information on status codes the Cisco NAC Web Agent passes back to the Cisco NAC Appliance system, see Table 11-5 in Cisco NAC Web Agent Status Codes, page 11-40.

12. The user can choose to do one the following:
    - Click **Continue** to complete Web Agent launch.
    - Click **Save Report** to save a local copy of the Web Agent session report that the user can forward on to the Cisco NAC Appliance administrator to help troubleshoot potential Web Agent login issues. The reports are available in the following formats:

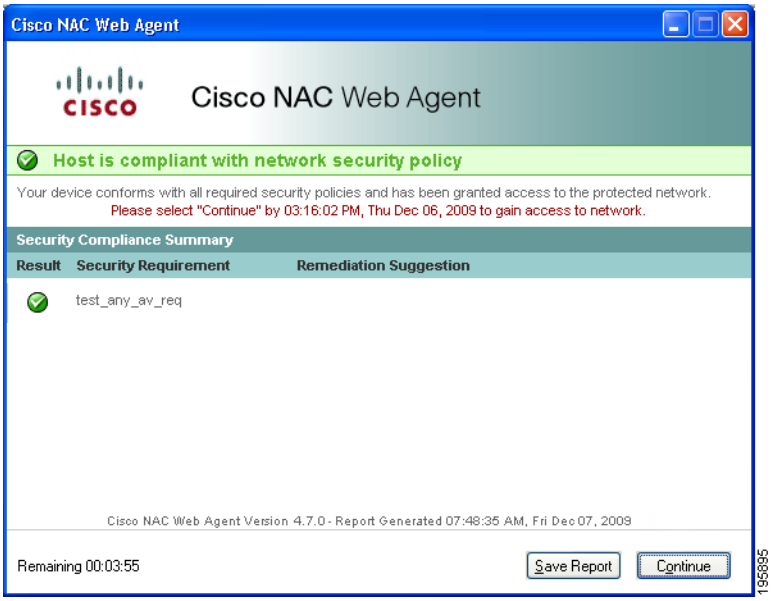
      Web Archive, Single File (*.mht)—Limited to the Microsoft Internet Explorer browser only

      Web Page, Complete (*.htm, html)—Supports any browser, but resource files (GIFs, CSS, etc.) are stored in a subdirectory

      Web Page, HTML Only (*htm, *.html)—Format and GIFs will not be present

      Text File (*.txt)

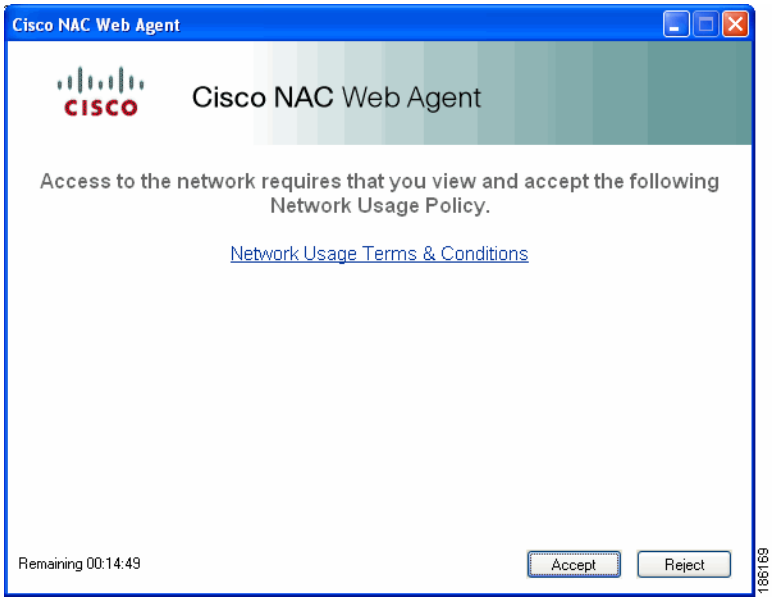
Figure 10-52 Requirement Met


Cisco NAC Web Agent
Cisco NAC Web Agent
Host is compliant with network security policy
Your device conforms with all required security policies and has been granted access to the protected network.
Please select "Continue" by 03:16:02 PM, Thu Dec 06, 2009 to gain access to network.
Security Compliance Summary
Result
Security Requirement
Remediation Suggestion
test_any_av_req
Cisco NAC Web Agent Version 4.7.0 - Report Generated 07:48:35 AM, Fri Dec 07, 2009
Remaining 00:03:55
Save Report
Continue
195895

13. If you have configured the Cisco NAC Appliance system to require the user to view and accept a Network Usage Policy guideline in the **Device Management > Clean Access > General Setup > Agent Login** page and have configured the **Device Management > Clean Access > Clean Access Agent > Installation** page to show the user the **Full UI** Direct Installation Option, the user may see a dialog similar to Figure 10-53. If the user does not accept the Network Usage Policy, the installation process halts and the user must choose to either restart the install and launch process or accept "restricted" network access.

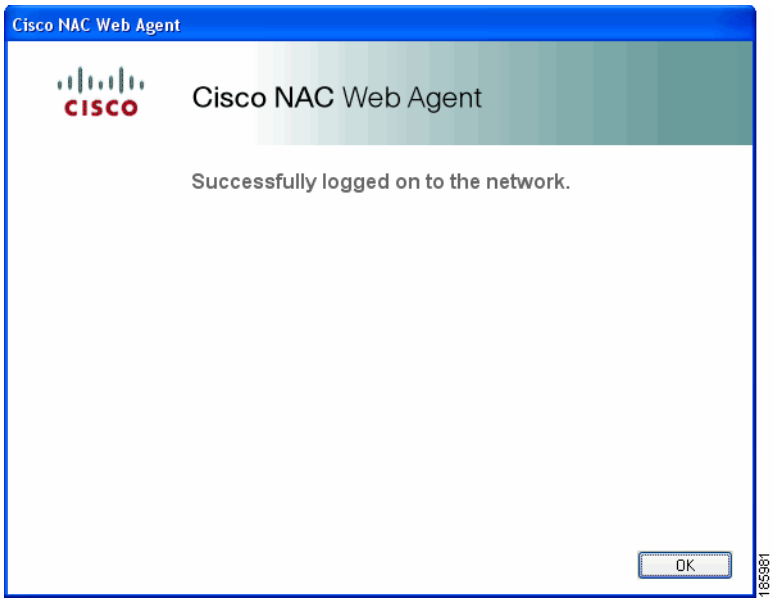
Note The first time users launch the Cisco NAC Web Agent on a client machine, they will likely see a pop-up blocker message at the top of the browser window after clicking "Accept" to continue past the Network Usage Policy.

Figure 10-53 (Optional) Network Usage Policy Dialog


Cisco NAC Web Agent
Cisco NAC Web Agent
Access to the network requires that you view and accept the following Network Usage Policy.
Network Usage Terms & Conditions
Remaining 00:14:49
Accept
Reject
186169

14. Once the user has performed manual remediation and successfully "re-scanned" the client machine, accepted any optional Network Usage Policy, identified and noted optional requirement items, or has chosen to accept "restricted" access for this user login session, the user receives a "Successfully logged on to the network" dialog (Figure 10-54) followed by a Clean Access Authentication browser window (Figure 10-56) featuring Web Agent session status information and a **Logout** button the user can click to terminate the Web Agent session.

Figure 10-54 Successful Cisco NAC Web Agent Login



It is possible that, even after the Cisco NAC Web Agent launched, installed, and initiated a login session without any issues, or that following manual remediation, the user was able to bring the client machine into compliance and successfully "re-scan" the client, another issue might keep the Cisco NAC Web Agent from logging the user into the network, resulting in a "You will not be allowed to access the network..." message similar to that in Figure 10-55. A couple of examples of known causes for this situation is a previous Web Agent session for the same user that did not "tear down" properly, on the CAM or if the user is currently logged into an active Cisco NAC Agent session.

If you receive one of these messages, click **OK** and attempt to launch the Cisco NAC Web Agent again. If the problem persists, contact your Cisco NAC Appliance system administrator.

Figure 10-55 Cisco NAC Web Agent Login Failed

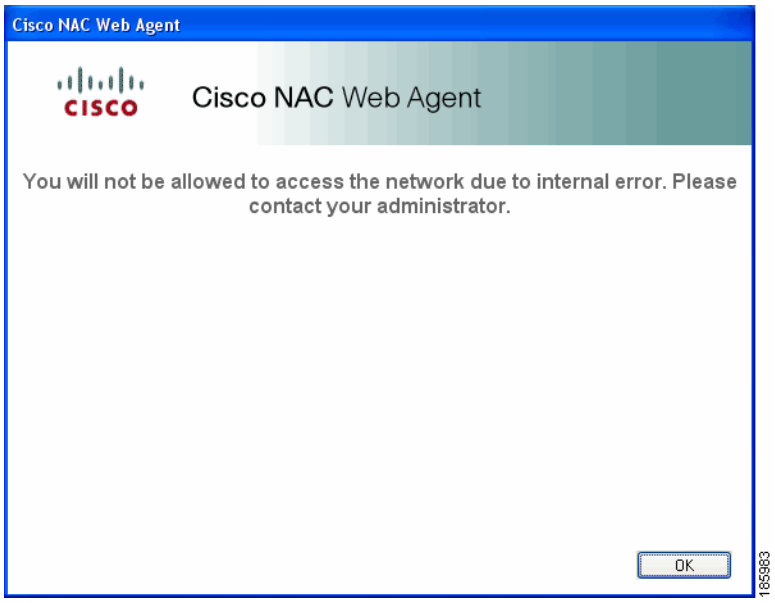

Cisco NAC Web Agent
Cisco NAC Web Agent
You will not be allowed to access the network due to internal error. Please contact your administrator.
OK
185983

Figure 10-56 Cisco NAC Web Agent Connection Status Window (Including Logout Button)


https://10.201.5.120 - Cisco Clean Access Authentication ...
File Edit View Favorites Tools Help
Cisco Clean Access Authentication
[Logon Information]
You have been successfully logged on the network.
http://192.168.241.31/
Time Logged on: 07/25/11 15:41:41
User Session: unlimited
[Logout Information]
To log yourself off the network, please click on the logout button.
Logout
Done
Internet
300118

15. To logout of the Cisco NAC Appliance user session and disengage the Cisco NAC Web Agent, the user clicks the **Logout** button. The web interface logs the user out of the network, removes the session from the client machine, and the user ID disappears from the Online Users list.

Note To log off the network and disengage the Cisco NAC Web Agent, the user can also right-click a Agent icon in the system tray and select **Logout**.

If you close the Web Agent connection browser window without "logging out" of the system, the user session remains active with the assigned user role until the CAM detects that the client machine is not longer available, a session timeout occurs, or some other event takes place to reveal the correct client machine state.

Note The administrator can configure the Web Agent Login success dialog to close automatically after a specified number of seconds, or not to appear at all. See Agent Login, page 1-7 for details.

Mac OS X Cisco NAC Agent

This section describes how to configure the Mac OS X Cisco NAC Agent to allow users to log in to the internal network via a persistent network access application installed on the client machine.

- Mac OS X Cisco NAC Agent Overview, page 10-44
- Configuration Steps for the Mac OS X Cisco NAC Agent, page 10-45
- Mac OS X Cisco NAC Agent Configuration File Settings, page 10-45
- Mac OS X Posture Assessment Prerequisites/Restrictions, page 10-45
- Requirement Types Supported for Mac OS X Agent, page 10-49
- Mac OS X Cisco NAC Agent Dialogs, page 10-50
- Mac OS X Cisco NAC Agent Application File Locations, page 10-63

Mac OS X Cisco NAC Agent Overview

The Mac OS X Cisco NAC Agent provides local-machine Agent-based posture assessment and remediation for client machines. Users download and install the Agent (read-only client software), which can check the host registry, processes, applications, and services.

After users log into the Cisco NAC Agent, the Agent gets the requirements configured for the user role/operating system from the Clean Access Server, checks for the required packages and sends a report back to the CAM (via the CAS). If requirements are met on the client, the user is allowed network access. If requirements are not met, the Agent presents a dialog to the user for each unmet requirement. The dialog (configured in the New Requirement form) provides the user with instructions and the action to take for the client machine to meet the requirement.

Mac OS X Cisco NAC Agent posture assessment is configured in the CAM by creating requirements based on rules and (optionally) checks, then applying the requirements to user roles/client operating systems. For more information, see Configuring Agent-Based Posture Assessment, page 9-39.

Note In the CAM web console, you can view the distribution options for the Mac OS X Cisco NAC Agent under **Device Management > Clean Access > Clean Access Agent > Distribution**. See Agent Distribution, page 9-18 for details.

Configuration Steps for the Mac OS X Cisco NAC Agent

The basic steps needed to configure the Mac OS X Cisco NAC Agent are as follows:

1. Make sure to follow the steps in Agent Configuration Steps, page 9-3 to enable distribution and download of the Mac OS X Cisco NAC Agent, including Require Agent Login for Client Machines, page 9-3 and Setting Up Agent Distribution/Installation, page 9-17.
2. Configure Mac OS X Agent requirements using the instructions in Configuring Agent-Based Posture Assessment, page 9-39:
   a. Configuring AV/AS Definition Update Requirements, page 9-41
   b. Configuring Custom Checks, Rules, and Requirements, page 9-70
   c. Map Requirements to Rules, page 9-90
   d. Apply Requirements to User Roles, page 9-92
   e. Validate Requirements, page 9-93
   f. Configuring an Optional/Audit Requirement, page 9-94

Mac OS X Cisco NAC Agent Configuration File Settings

This Mac OS X Cisco NAC Agent features can be configured and enabled by setting the parameters in the following files:

- **~/Library/Application Support/Cisco Systems/CCAAgent/preference.plist**
- **/Applications/CCAAgent/Contents/Resources/setting.plist**

Table 10-1 lists the configuration parameters that are supported.

Mac OS X Posture Assessment Prerequisites/Restrictions

Macintosh Client machines and the CAM/CAS must meet the following requirements to be able to perform posture assessment using the Mac OS X Cisco NAC Agent.

Mac OS X Agent Prerequisites

- The Mac OS X Agent installer (built by Apple's "Package Maker" system application) installs two application files on the client: **CCAAgent.app** to launch the Mac OS X Cisco NAC Agent, and **dhcp_refresh** to facilitate IP address refresh procedures.
- The client machine must be running the most recent release of 10.5 (release 10.5.2) or later to support Macintosh client posture assessment. Mac OS 10.2 and 10.3 do not support posture assessment and remediation. For more information, see *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.
- Auto-upgrade of the Mac OS X Agent is supported starting from version 4.1.3.0 and later in Cisco NAC Appliance. Users can upgrade client machines to the latest Mac OS X Agent by downloading the Agent via web login and running the Agent installation. For more information, see the corresponding *Release Notes for Cisco NAC Appliance*.
- When a Link Distribution requirement type launches a browser, it uses the default browser which the user can configure in their Safari browser's **Preference** settings. The user can pick any browser they like, including Safari, Firefox, or Opera.

- The Mac OS X Agent fully supports UTF-8. Therefore, if a requirement from the CAM is configured in any language other than English (like Traditional Chinese, for example), the Mac OS X Agent is still able to display Agent text correctly. The administrator just needs to create a different user interface file (.nib) using Apple's Interface Builder and change the locale in the client machine's System Preferences, No code is required to implement this feature.

  To localize the user interface:

  a. Add a new localized .nib file in the Interface Builder and re-compile the Mac OS X Agent (zh_TW is the language code for Traditional Chinese).

  b. Change the locale in the client machine's System Preferences.

  c. The Mac OS X Agent then displays the localized user interface based on the new locale setting.

- User Preference configuration options (~/Library/Application Support/Cisco Systems/CCAAgent/preference.plist):

  a. Suppress auto-popup the login window when detecting the CAS.

  b. Allow saving user's credential in the memory until quitting the agent.

  c. Change the VLAN detection interval (default is 5 seconds, 0 is disable).

In Release 4.9 and later, the VLAN Detect is automatically disabled when the client machine is on VPN connection. The following VPN clients are supported:

- Cisco VPN Client
- AnyConnect
- Apple Native VPN Client to Cisco IPSEC
- Shimo(User Interface for Cisco IPSEC client)

Note The Mac Agent automatically creates a **preference.plist** file when either or both of the "Auto Popup Login Window" or "Remember Me" options are toggled for the Mac Agent. If neither of these options are changed for the Agent, the user would have to manually produce a preference.plist file on the Mac OS X client machine.

Example preference.plist File Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>AutoPopup</key>
    <string>yes</string>
    <key>RememberMe</key>
    <string>yes</string>
    <key>VlanDetectInterval</key>
    <string>5</string>
</dict>
</plist>
```

Note Refer to Table 10-1, for more details on all the configuration parameters.

- Agent Setting configuration options are done in the **/Applications/CCAAgent/Contents/Resources/setting.plist.** The **setting.plist** is used to configure the parameters globally for all the users except the "RememberMe" and "AutoPopup" options.

Example setting.plist File Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>RetryDetection</key>
    <string>3</string>
    <key>PingArp</key>
    <string>2</string>
    <key>LogFileSize</key>
    <string>5</string>
</dict>
</plist>
```

Note Refer to Table 10-1, for more details on all the configuration parameters.

Table 10-1 Mac OS X Cisco NAC Agent Configuration Parameters

Parameter	Default Value	Valid Range	Description/Behavior
RememberMe [1]	yes	yes or no	If this setting is **yes**, the user only needs to enter login credentials once. The Mac OS X Agent also remembers the user credentials after session termination/time-out. **Note** When the user logs out of Windows, the saved credentials are erased. When the user moves from a connection that requires username and password to an SSO session and returns back, then the credentials are removed.
AutoPopup [1]	yes	yes or no	• If this setting is **yes**, the Agent login dialog appears automatically when the user is logged out. • If this setting is **no**, users must manually initiate login using the Tools menu option.
LogFileSize	5	0 and above	This setting specifies the file size (in Megabytes) for Mac OS X Agent log files on the client machine. • If this setting is **0**, the Agent does not record any login or operation information for the user session on the client machine. • If the administrator specifies any other integer, the Agent records login and session information up to the number of MB specified.

Table 10-1 Mac OS X Cisco NAC Agent Configuration Parameters (continued)

Parameter	Default Value	Valid Range	Description/Behavior
DiscoveryHost	—	IP address or FQDN	This setting specifies the Discovery Host address the Agent uses to connect to the Cisco NAC Appliance system in a Layer 3 deployment.
RetryDetection	3	0 and above	If ICMP or ARP polling fails, this setting configures the Agent to retry <*x*> times before refreshing the client IP address.
HttpDiscoveryTimeout	5	3 and above	The default timeout is 5 seconds. This is the time for which the HTTPS discovery from Agent waits for the response from Clean Access Server. If there is no response for the specified time, then the discovery is timed out. The minimum value that can be set is 3. If the value is set to 1 or 2, the timeout is recognized as 3 seconds. If this value is set to zero (0), then the Windows default timeout settings are used.
HttpTimeout	5	3 and above	The default timeout is 120 seconds. This is the time for which the HTTP request from Agent waits for the response. If there is no response for the specified time, the request is timed out. The minimum value that can be set is 3. If the value is set to 1 or 2, the timeout is recognized as 3 seconds. If this value is set to zero (0), then the Windows default timeout settings are used.
PingArp [2]	2	0-2	• If this value is set to **0**, poll using ICMP. • If this value is set to **1**, poll using ARP. • If this value is set to **2**, poll using ICMP first, then (if ICMP fails) use ARP.
PingMaxTimeout	1	1-10	Poll using ICMP and if no response in <*x*> seconds, then declare ICMP polling as failure.
VlanDetectInterval [3,4]	5	5-900	• If this setting is **0**, the Access to Authentication VLAN change feature is disabled. • By default, this setting is **5** and the Agent sends ICMP/ARP queries every 5 seconds. • If this setting is **6-900**, ICMP/ARP every <*x*> seconds.

1. The RememberMe and the AutoPopup parameters can be set only in the **preference.plist** file.
2. If the PingArp value is "1", it breaks the VPN connections by removing the Gateway entry. If the value is "0", then it breaks network connections with Managed subnets on In Band. It is recommended to have the value as “2”.

3. In Release 4.9 and later, the VLAN Detect is automatically disabled when the client machine is on VPN connection. The following VPN clients are supported:
   - Cisco VPN Client
   - AnyConnect
   - Apple Native VPN Client to Cisco IPSEC
   - Shimo(User Interface for Cisco IPSEC client)
4. During the discovery, all the VLAN Detect parameters are set to their default values and these values cannot be overridden. The parameters are: **RetryDetection, PingArp, PingMaxTimeout,** and **VlanDetectInterval**. Refer to Table 10-1 for the default values of these parameters.

Mac OS X Agent Restrictions

- The Mac OS X Cisco NAC Agent only supports a subset of the posture assessment functions available for the Windows Clean Access Agent. (Only Link Distribution, AV Definition Updates, AS Definition Updates, and Local Checks are supported.)
- The Mac OS X Agent does not support auto-remediation. The user must manually remediate all mandatory requirements to make the client machine compliant with network security guidelines.
- The Mac OS X Agent does not support IP-based certificates for authentication.
- The Log file (~/Library/Application Support/Cisco Systems/CCAAgent/event.log) is encrypted. Contact Cisco Technical Assistance Center for help with decryption.

CAM/CAS Restrictions

- Cisco NAC Appliance only supports 10.5 and later. Mac OS 10.2, 10.3, and 10.4 are not supported. For more information, see *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.
- The Mac OS X Agent does not support custom checks and custom rules. You can only assign AV and AS rules to the Link Distribution, Local Check, AV Definition Update, and AS Definition Update requirement types for Mac OS X posture remediation.
- You cannot configure the CAM to install the Mac OS X Agent using a stub installer.

Requirement Types Supported for Mac OS X Agent

The Mac OS X Cisco NAC Agent performs a subset of the posture assessment functions supported on the Windows Clean Access Agent. The posture assessment functions currently supported on the Mac OS X Agent are:

- **Link Distribution**—This requirement type refers users to another web page where the software is available, such as a software download page. Make sure the Temporary role is configured to allow HTTP (and/or HTTPS) access to the link.
- **Local Check**—This requirement type can be used to create checks that look for software that should or should not be on the client machine. For the Mac OS X Agent, Local Checks are used primarily as a message medium to inform users what to do if/when a particular rule has/has not been met. The Mac OS X Agent Assessment Report window displays Local Check requirements using a “Message” icon.

- **AV Definition** and **AS Definition Updates**—These requirement types are used to report on and update the definition files on a client for supported antivirus or antispyware products.

Note For a list of support AV/AS applications, see the "Clean Access Supported AV/AS Product List" section of the corresponding *Release Notes for Cisco NAC Appliance*.

- Although the Windows Agent supports "auto-remediation," Mac OS X Agent users must manually remediate their client machines to meet security requirements.

Mac OS X Cisco NAC Agent Dialogs

Note The Mac OS X Cisco NAC Agent supports single-sign on (SSO) with VPN deployments but does not support SSO with Active Directory.

See also the "SSL Requirements for Mac OS/CAS Communication" section in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for additional details.

The Mac OS X Cisco NAC Agent user sequence is as follows.

1. The user navigates to the untrusted interface address of the CAS and is redirected to the Login page (Figure 10-57).

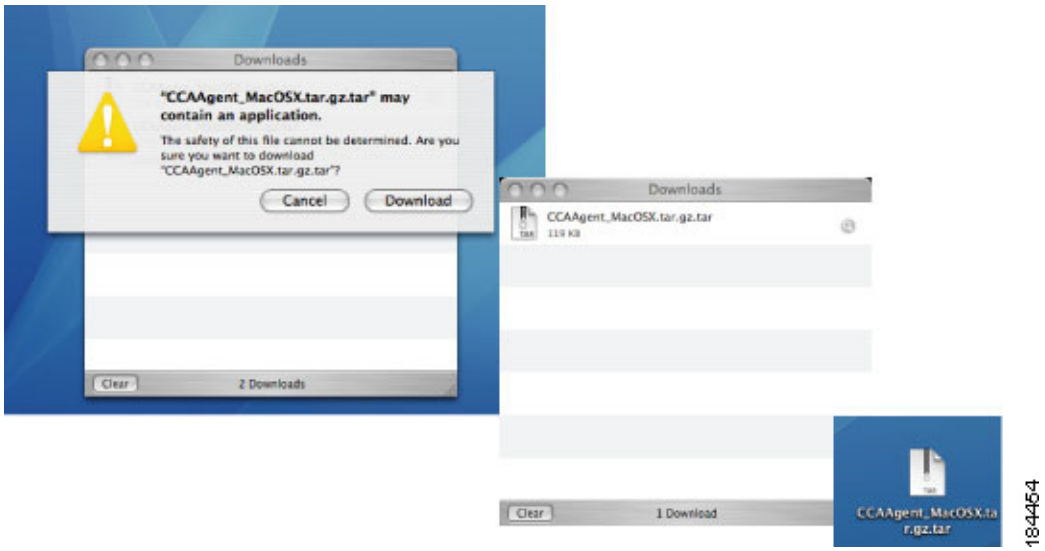
Figure 10-57 Login Page—Mac OS X



The user is directed to the Download Cisco NAC Agent page.

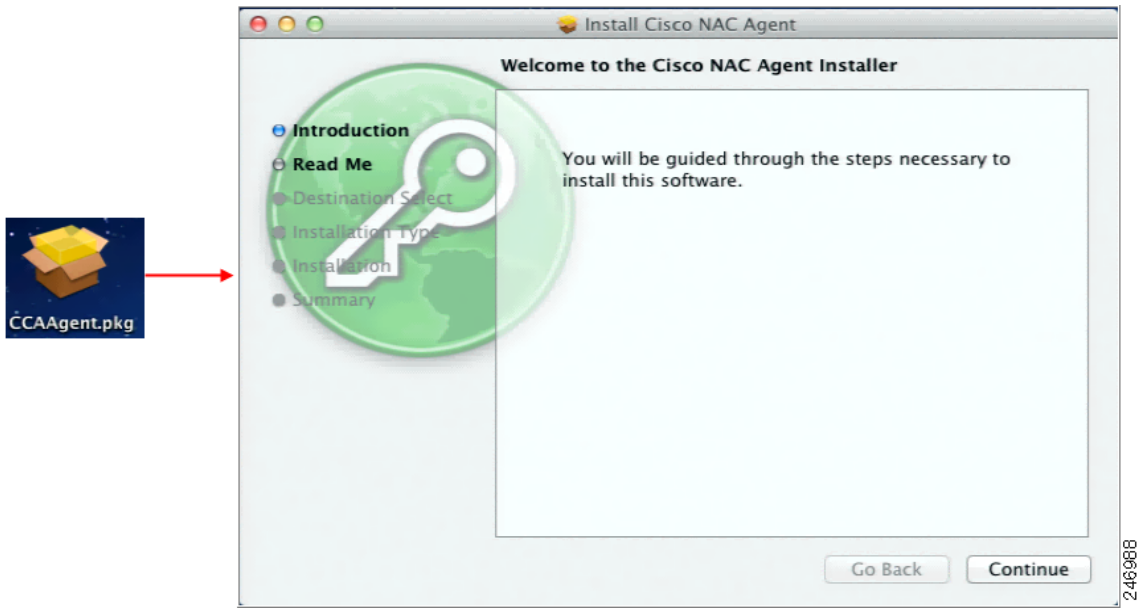
2. The user clicks the "Download" button and the CCAAgent_Mac OSX.tar.gz.tar file is download to the desktop (Figure 10-58) and untarred.

Figure 10-58 Download Cisco NAC Agent Setup Executable to Desktop



3. The user double-clicks the CCAAgent.pkg file and the Mac OS installer for the Cisco NAC Agent starts up (Figure 10-59).

Figure 10-59 Double-Click CCAAgent.pkg to Start Cisco NAC Agent Installer



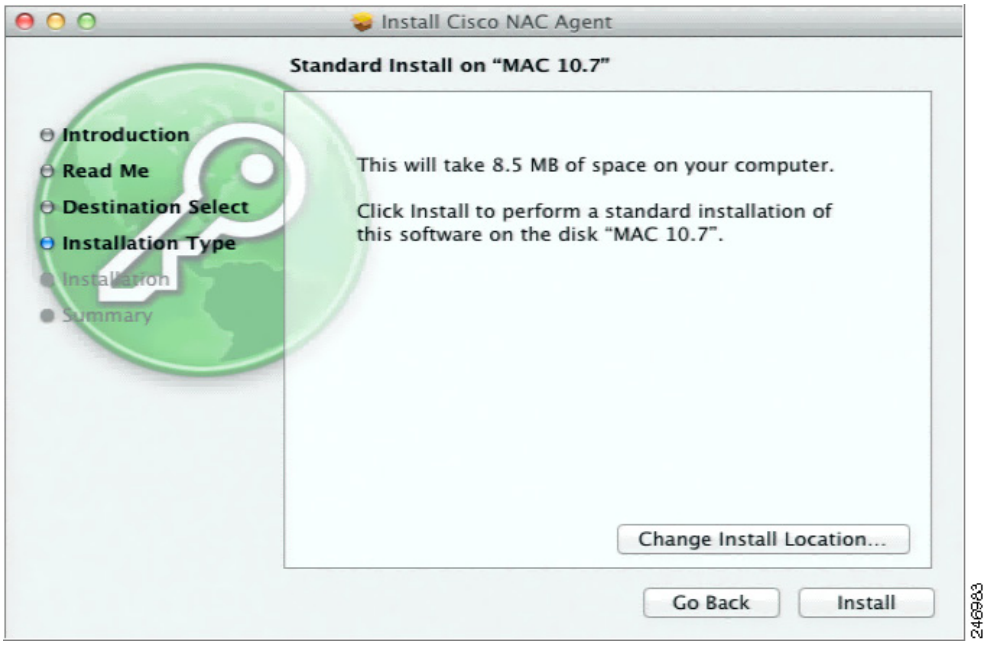
4. The user clicks the **Continue** button to proceed to the Read Me screen of the installer.

5. The user clicks the **Continue** button to proceed to the Select a Destination screen of the installer (Figure 10-60).

Figure 10-60 Mac OS X Agent Installation—Select a Destination



Figure 10-61 Mac OS X Agent Installation—Install/Upgrade Button



6. The user clicks the **Install/Upgrade** button to perform the installation (Figure 10-61). When done, the user clicks **Close**.

Note If the Cisco NAC Agent has never been installed on the machine, the Installation screen displays an **Install** button. If the Agent was installed at one point, even if there is no Agent currently in the system when the installer is invoked, the **Upgrade** button is displayed.

Figure 10-62 Mac OS X Agent Installation In Progress

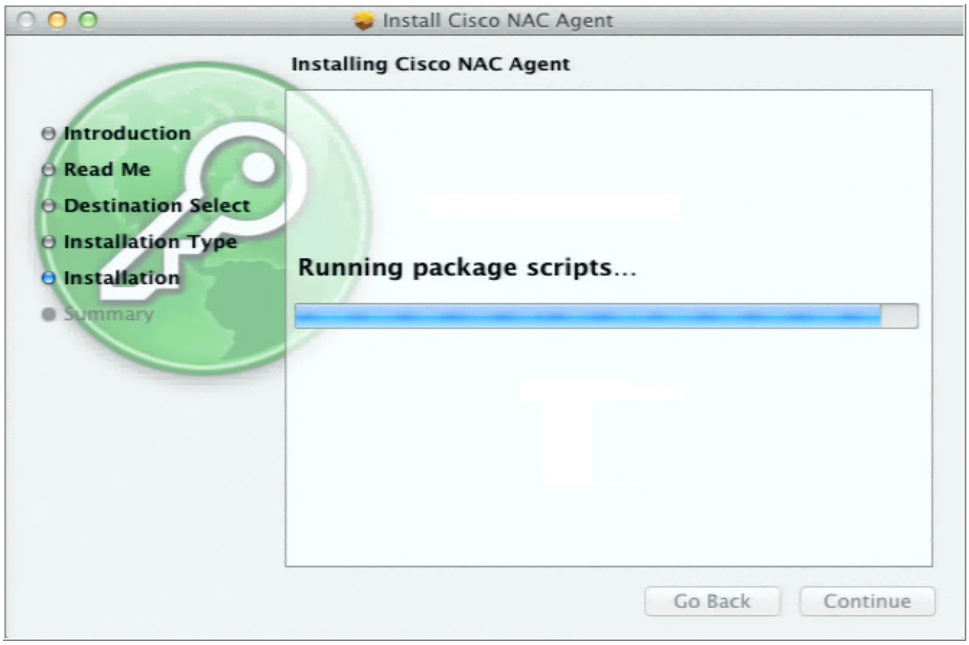
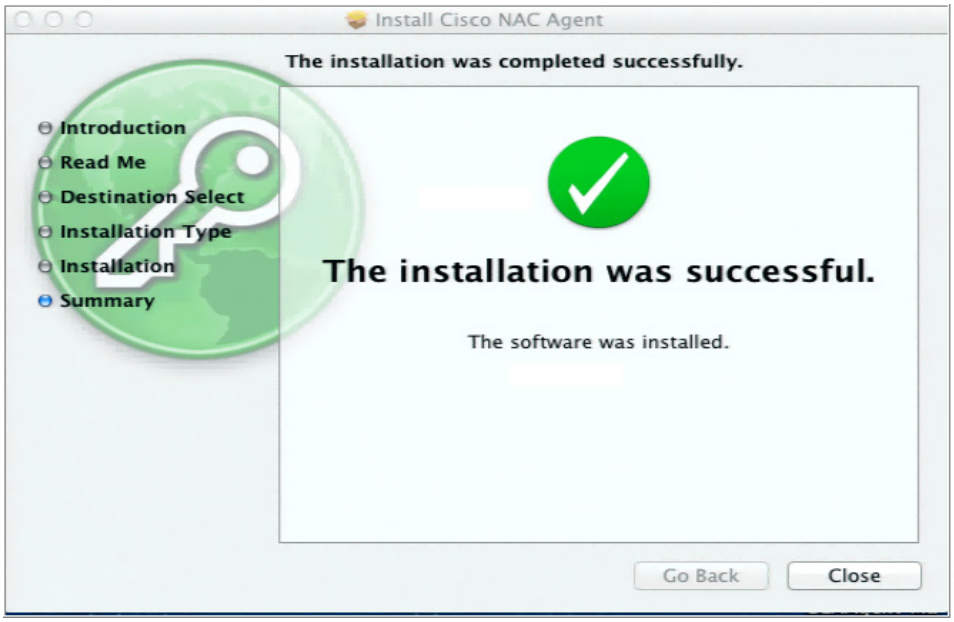


Figure 10-63 Mac OS X Agent Installation—Install Succeeded



7. After installation, the Cisco NAC Agent login dialog appears. The Agent icon is now available from the Tool Menu (Figure 10-64). Right-clicking the Agent icon brings up the menu choices:
   - **Login/Logout** (toggle depending on login status)

     Note If Cisco Clean Access employs a RADIUS server for user authentication and the server has been configured to authenticate users with additional credentials, the user may be presented with one or more additional challenge-response dialogs like those described in RADIUS Challenge-Response Mac OS X Cisco NAC Agent Dialogs, page 10-65.

   - **Auto Popup Login Window** (enabled by default)
   - **About** (displays version screen for the Cisco NAC Agent and the Compliance Module)
   - **Collect Support Logs** (collects logs and support information)

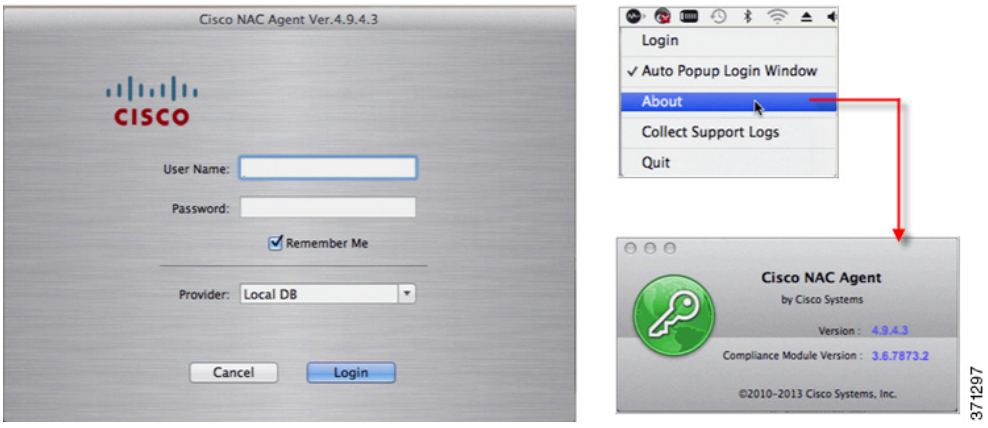
     The user can click the **Collect Support Logs** option to collect the Agent logs and support information. The collected information is available as a zip file (*CiscoSupportReport.zip*) on the desktop of the client machine. While collecting the support logs, if a file with same name is available on the desktop, the old file is deleted and new file will be created.

     If the Agent crashes or hangs, you can run the **CCAAgentLogPackager.app** to collect the logs. This file is available in the Applications folder where the Cisco NAC Agent has been installed. You can double click this file to collect the support information.

     Note The **Collect Support Logs** option is available only for Cisco NAC Appliance, Release 4.9(1) and later.

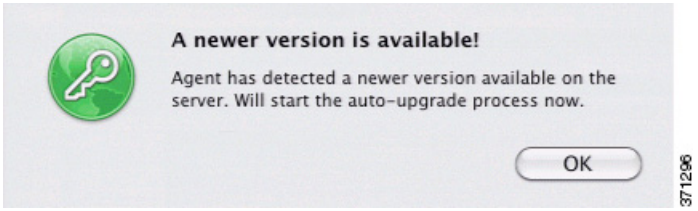
   - **Quit** (exits the Cisco NAC Agent application)

Figure 10-64 Cisco NAC Agent Login Pops Up/Desktop Icon Available from Tool Menu



8. **Auto-Upgrade for Already-Installed Agents**: When the Mac OS X Agent is already installed, users are prompted to auto-upgrade at each login, unless you disable upgrade notification. You can optionally force logout at machine shutdown (default is for users to remain logged in at machine shutdown). You can configure auto-upgrade to be mandatory or optional. With optional auto-upgrade and a newer version of the Agent available from the CAM, existing Mac OS X Agent users will see the following upgrade prompt at login (Figure 10-65).

Figure 10-65 Mac OS X Agent—New Agent Version Available


A newer version is available!
Agent has detected a newer version available on the server. Will start the auto-upgrade process now.
OK
371296

9. Clicking **OK** in the above dialog brings up the setup wizard to upgrade the Mac OS X Agent to the newest version. After Agent upgrade and user login, requirement checking proceeds. If the upgrade is optional and a newer version of the is Agent available from the CAM, users can choose to **Cancel** the upgrade and continue with the login process (Figure 10-66).
10. If the Compliance Module feature has been enabled, the users are prompted to install the Mac OS X Agent Compliance Module.
11. If the user clicks **Yes**, the Cisco NAC Agent is upgraded to the newest version of Mac OS X Agent Compliance Module automatically. The upgrade happens at the background and after successful upgrade, the agent will proceed to login. The user is notified if there is an error in download or upgrade.
12. The user provides authentication credentials in the Mac OS X Agent login dialog to sign in to the Cisco NAC Appliance system.

Figure 10-66 Mac OS X Agent Login Dialog



13. During login, the Mac OS X Agent icon in the Macintosh client machine menu bar at the top of the Macintosh desktop displays differently based on the relative status and segment of the login process:
    a. **Searching**—The Agent is not currently connected and is in the process of transmitting SWISS packets to discover the CAS.



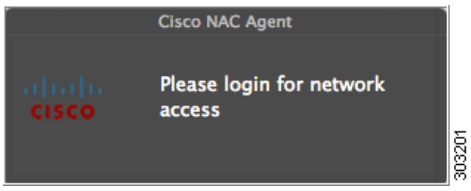
b. **Ready and waiting**—The Agent is connected to the CAS and ready to log in.



c. **Lost focus**—When the Agent window is not the top application on the desktop, the status icon shows “CLICK” and “FOCUS” repeatedly. Once the user clicks on the status icon, the Agent window becomes the active window on the desktop. This signal is helpful when the Agent window is “buried” by several other windows or applications, especially when a link remediation pops up a browser on top of the Agent and the user wants to switch back to the Agent after downloading an application or update.

   When "Login" or "Remediation" window is displayed, the Agent waits for user-action. At this time, if the Agent window loses focus or "buried" by other windows, then a notification screen pops-up at the right-bottom corner as shown below.





d. **Quarantined**—If the Agent is in the Temporary role during posture assessment and remediation, the menu bar displays this icon to tell the user that they only have limited access to the network.



e. **Logged in**—The user has completed the login process and is ready to use the network.



f. **Logged in via VPN**—The user is signed in via a VPN or VPN SSO connection and has been successfully logged in.



g. **Error**—When an error occurs (for example, if the client cannot validate the CAS certificate, sees an invalid CAS certificate, or domain name resolution fails) the status icon changes to the exclamation point (!) icon.



14. Following user log in, if any mandatory or optional requirements fail, the user is assigned to the default Temporary role and sees the Assessment Report window (see Figure 10-67) containing the following information for each requirement in the report:

- **Run**—This column either contains a checkbox that the user can choose to check or leave unchecked (if the requirement is optional), or a "grayed-out" checkbox (if the requirement is mandatory). This enables the user to select the optional requirements to remediate *before* clicking the **Remediate** button to address all requirements listed in the Assessment Report window.
- **Name**—This is the name of the requirement the administrator configures on the CAM.
- **Description**—This field contains text from the "Description" field the administrator enters in the CAM when configuring the requirement to provide information/explanation.
- **Type** (icons)—The icons in this column denote the requirement type ("Link," "Update," or "Message").
- **Required**—Specifies whether the requirement is **Mandatory** or **Optional**.

  If there are **Mandatory** requirements associated with the user login session that do not pass upon posture assessment, the Mac OS X Agent automatically displays the Assessment Report dialog after the user enters login credentials.

  If the only requirements that fail are **Optional** requirements, the Agent still displays the Assessment Report dialog to the user, but they are allowed to click the **Complete** button and successfully log in to the network. (In this situation, the Agent assumes that all **Mandatory** requirements (if any) have passed and the user has a choice to remediate or log in.)

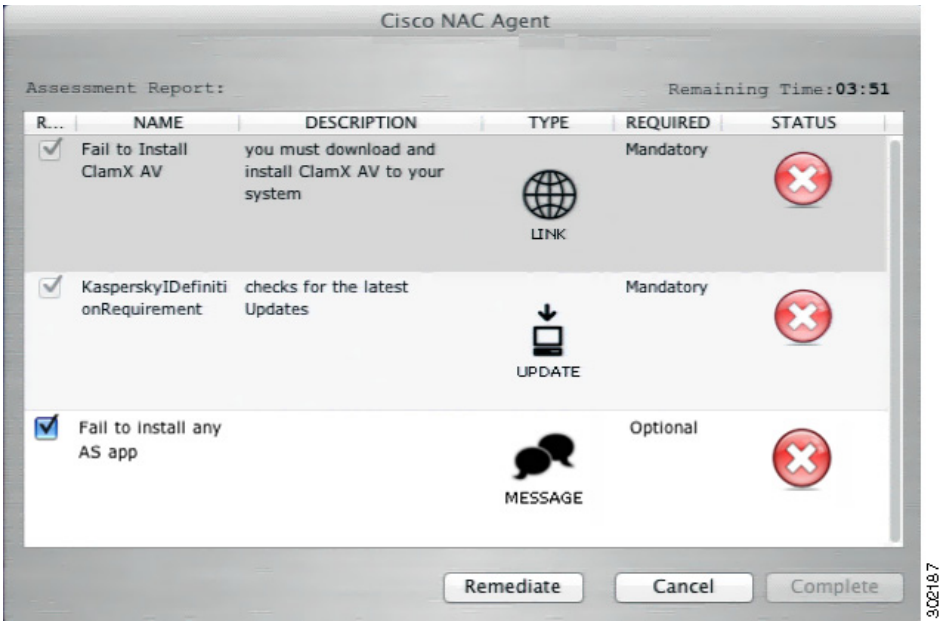
  Note Audit requirements are always checked/verified in the background and do not appear in the user-facing Assessment Report window with "failed" mandatory or optional requirements.

- **Status** (icons)—Displays the current status of the requirement type in the report dialog. When an assessment dialog first opens, all of the requirement types in the report are "failed" (denoted by an "X" icon). As the user addresses each requirement in turn, the status icons can change to "passed" (denoted by a checkmark icon), or "Skip" in the case of optional requirement types or mandatory requirements that the user could not remediate at that time.

  Note If a user chooses to "Skip" a mandatory requirement, they are able to progress through and address the other requirement types/entries in the Assessment Report, but cannot log into the network until they have successfully remediated their client machine and passed all of the mandatory requirements. (See Figure 10-70.)

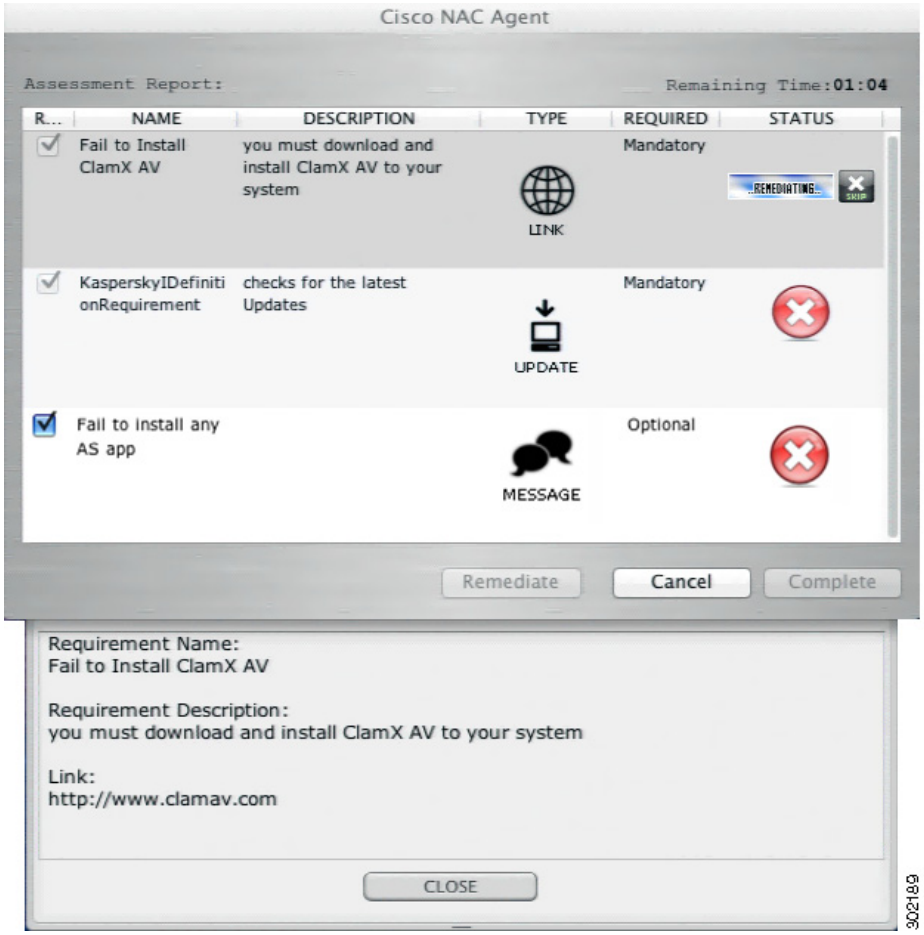
The Assessment Report window also displays the time remaining (in the upper right corner) before the Agent Temporary role expires and the client remediation window closes, requiring the user to log in and resume remediation again.

Figure 10-67 Mac OS X Agent Assessment Report Dialog



15. The user clicks the **Remediate** button to begin updating the client machine to meet the requirement criteria. The Mac OS X Agent begins the remediation process on the first "failed" requirement in the Assessment Report, and progresses through the requirement list one-by-one until all of the requirements in the list either "pass" posture assessment or the user "skips" one or more mandatory requirements. Depending on the type of requirement, the user sees one of the following processes during the remediation process:
    - In the case of a Link Distribution ("Link") requirement, users are directed to a web page, such as a software download page, where the required software is available and the user can quickly begin the download and installation process.
    - In the case of a Live Definition Update ("Update") requirement, the Mac OS X Agent reports on and (once the user clicks **Remediate**) automatically updates the definition files on the client machine for supported antivirus or antispyware products.
    - In the case of a Local Check ("Message"), the Mac OS X Agent looks for software that should or should not be installed on the system. (In the context of the Mac OS X Agent, this feature is used primarily as a message medium to inform users what to do if/when a particular rule has/has not been met. The user does not undertake any specific action in the Assessment Report window, itself.)
16. During requirement remediation, a user can choose to bypass mandatory requirements when the **Skip** button appears in the **Status** column. (See Figure 10-68.) If the user clicks **Skip** in this scenario, they cannot log into the Cisco NAC Appliance system, as the mandatory requirement has not been satisfied. This function can be useful for users who know that a particular mandatory requirement cannot succeed within the time constraints of the Temporary role and they want to move on to other more easily-manageable mandatory requirements.

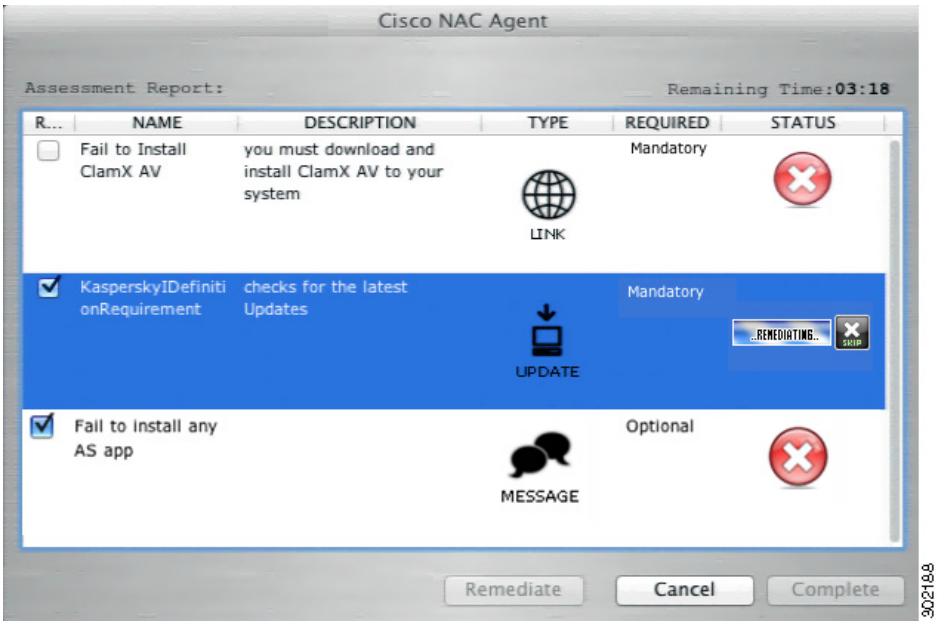
Figure 10-68 Mac OS X Agent Requirement Resolution



If the Name and/or Description for a given requirement are too long to display completely in the Assessment Report window, users can still view the complete text in a pop-up (or "drawer") that appears in addition to the Assessment Report.

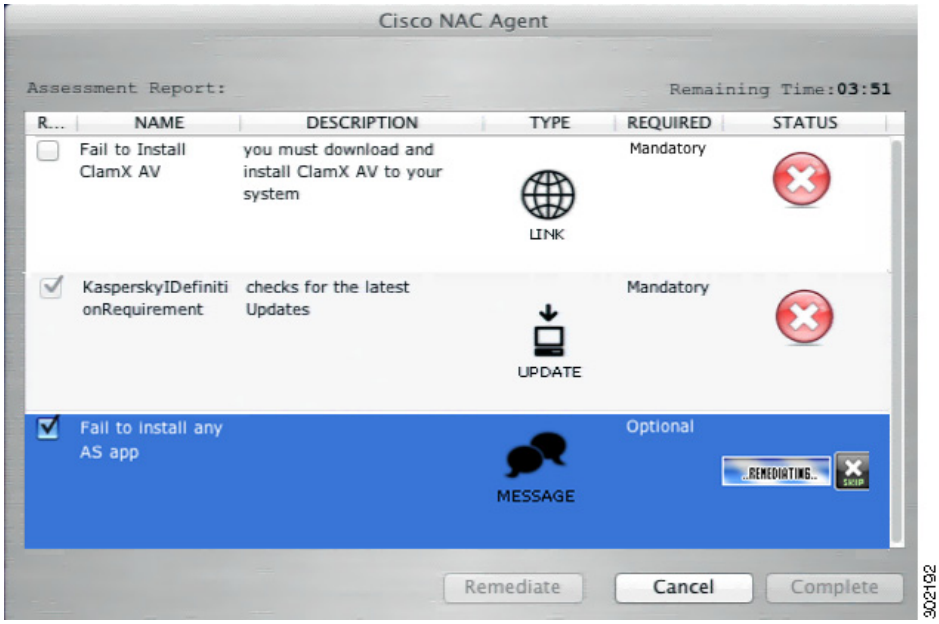
17. If an error occurs during remediation, the Assessment Window displays the error message text above the requirement list. For example, Figure 10-69 displays an error that occurred during the mandatory live definition update reading, "No product that supports def-update found!"

Figure 10-69 Mac OS X Agent Requirement Failed



If one or more mandatory requirements still fail following the remediation process, the user can only choose **Cancel** in the Assessment Report window and cannot log into the Cisco NAC Appliance system. (See Figure 10-70.)

Figure 10-70 Previous Mac OS X Agent Mandatory Requirement(s) Failed



18. Users can also choose to "Skip" optional requirements in the Assessment Report (see Figure 10-71). If users click **Skip**, the Status icon turns to "fail" (the "X" icon) as shown in Figure 10-72, but the user is still allowed to log in to the system because the requirement is optional instead of mandatory.

Figure 10-71 Mac OS X Agent Optional Requirement

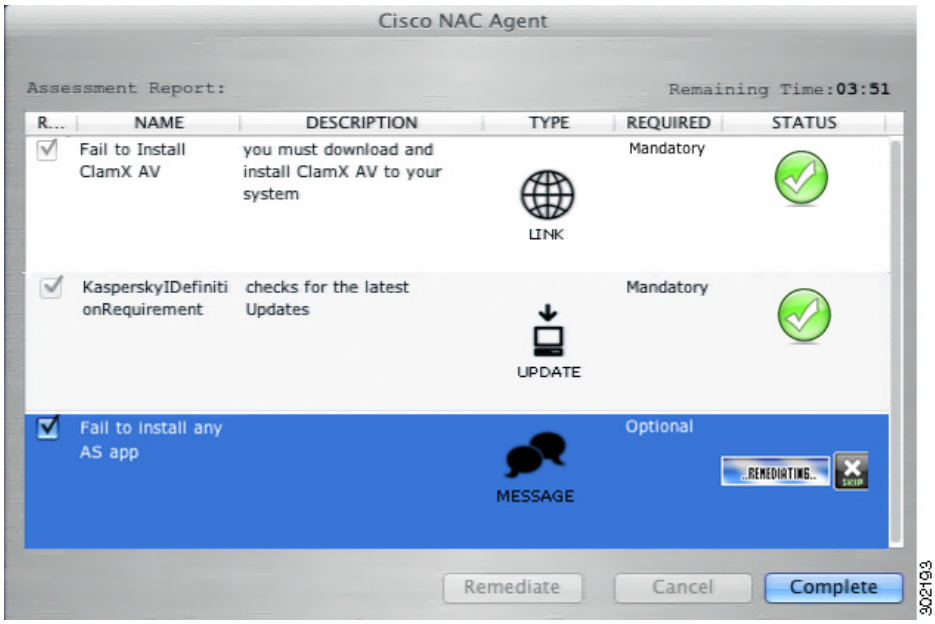
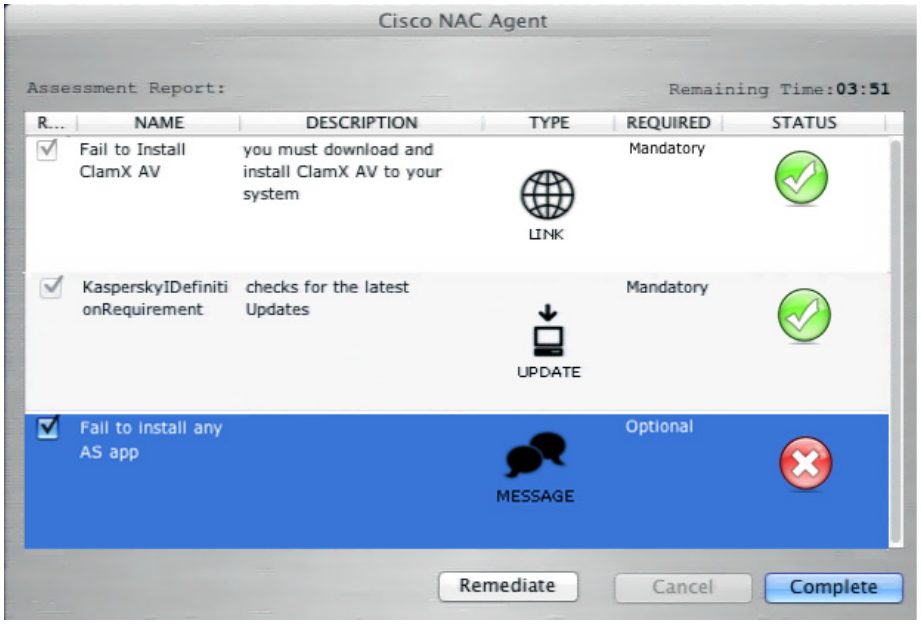
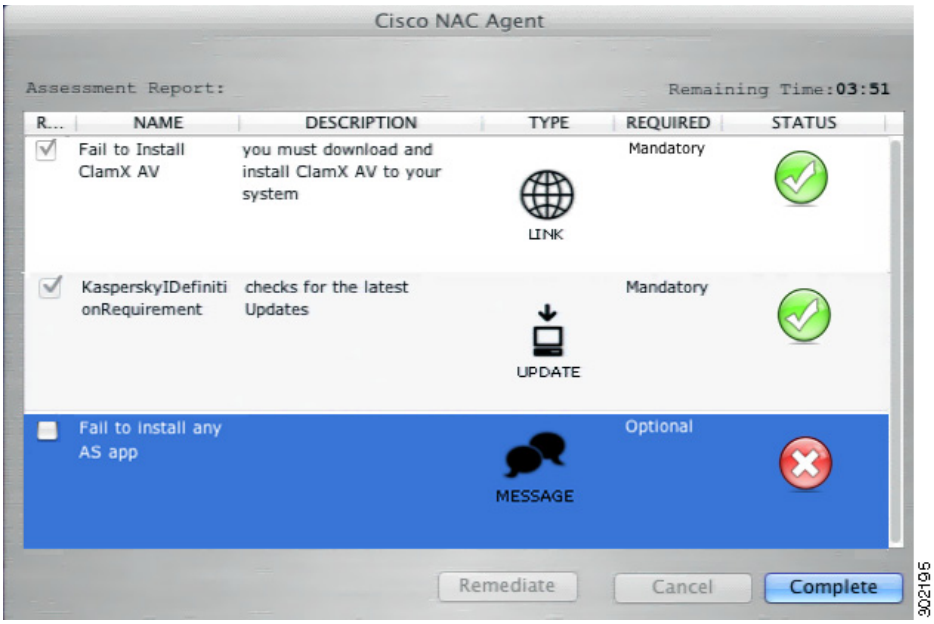


Figure 10-72 Mac OS X Agent Optional Requirement Failed



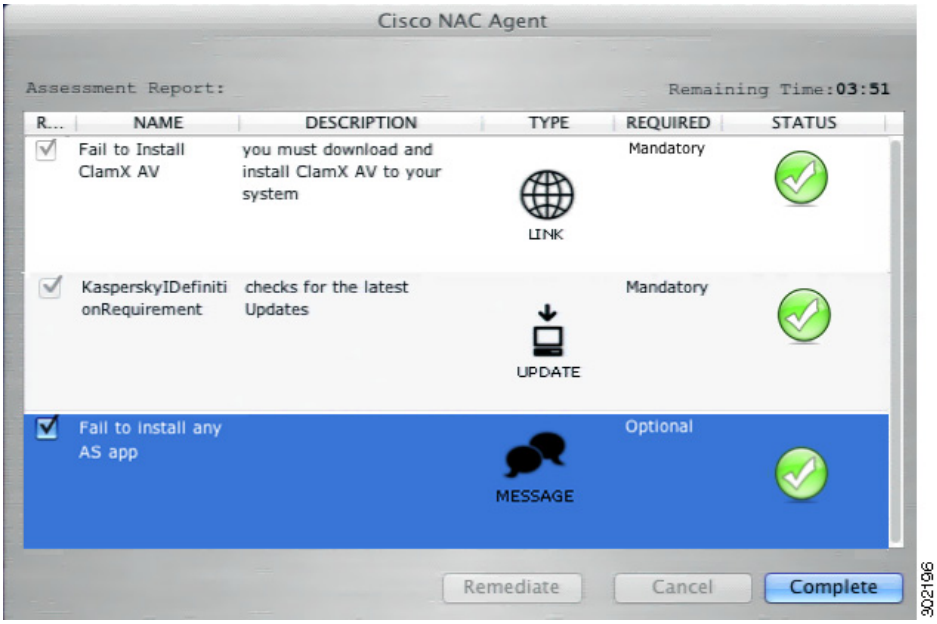
The Mac OS X Agent behaves similarly if the user chooses not to perform remediation for an optional requirement type by disabling the particular requirement entry before clicking the **Remediate** button (see Figure 10-73). When the Agent reaches this particular requirement in the Assessment Report window, the Agent automatically marks the requirement "failed" and either moves on to the next requirement, or (if the optional requirement is the last in the list and all other requirements have been met) displays the **Complete** button.

Figure 10-73 Mac OS X Agent Optional Requirement Skipped



19. When all requirements pass remediation, the user sees the **Complete** button at the bottom of the Assessment Report window and can log into the Cisco NAC Appliance system. (See Figure 10-74.)

Figure 10-74 All Mac OS X Agent Requirements Passed



20. The user clicks the **Complete** button once all mandatory requirements are met and successfully logs into the network. Once the user successfully logs into the Cisco NAC Appliance system, the Mac OS X Agent sends an Assessment Report back to the CAS.

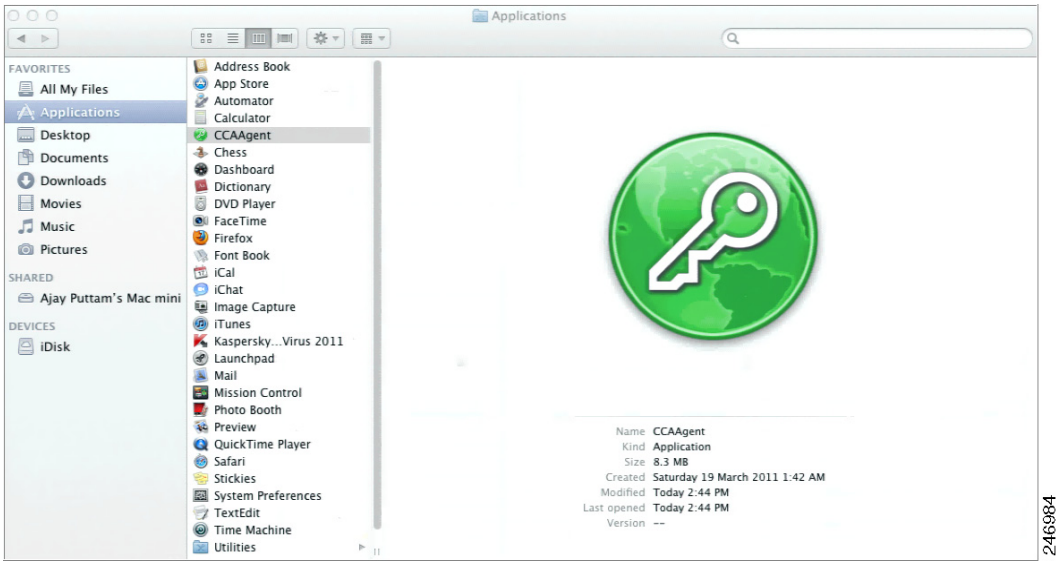
Figure 10-75 Mac OS X Agent Login Successful



Mac OS X Cisco NAC Agent Application File Locations

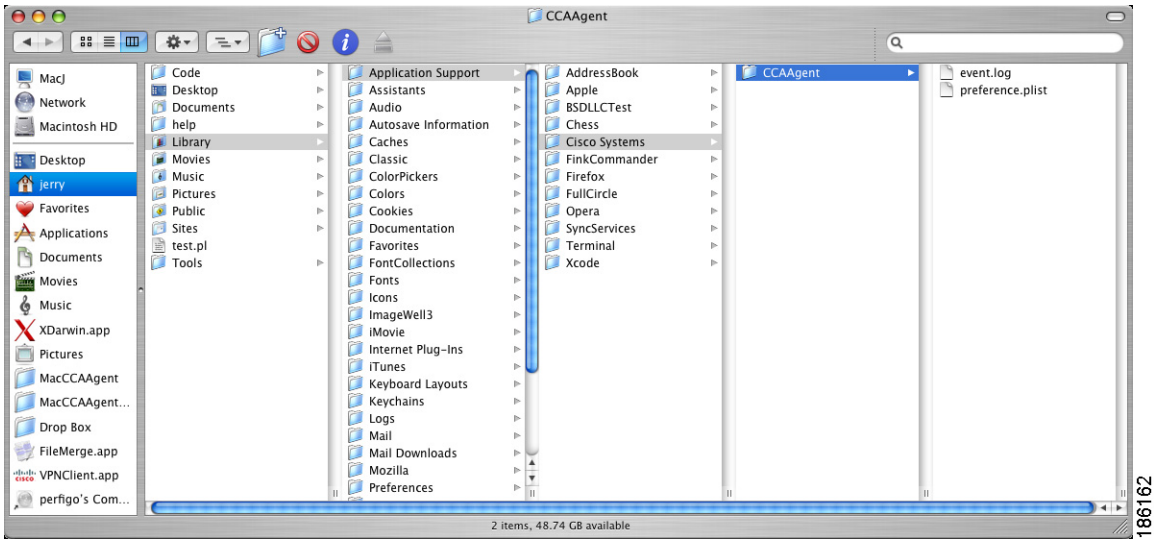
The Cisco NAC Agent application itself is installed under **Macintosh HD > Applications > CCAAgent.app** (Figure 10-76).

Figure 10-76 Cisco NAC Agent—Application Installation Location



The Cisco NAC Agent **event.log** debug file and **preference.plist** user preferences file are installed in the **<username> > Library > Application Support > Cisco Systems > CCAAgent** folder (Figure 10-77).

Figure 10-77 Cisco NAC Agent—event.log and preference.plist File Locations

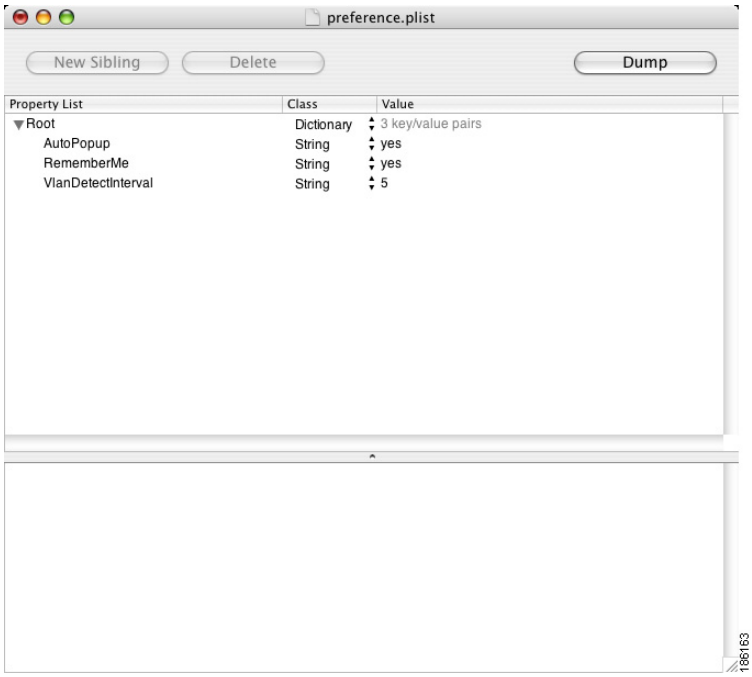


The **preference.plist** file (Figure 10-78) includes:

- Whether **AutoPopup Login Window** is checked in the Menu (AutoPopup).
- Whether **Remember Me** is checked in the Login screen (RememberMe).
- How frequent the agent will perform Access to Authentication VLAN change detection (VlanDetectInterval).

Note The Mac Agent automatically creates a **preference.plist** file when either or both of the "Auto Popup Login Window" or "Remember Me" options are enabled for the Mac Agent. If neither of these options are enabled for the Agent, the user would have to manually produce a preferences.plist file on the Mac OS X client machine.

Figure 10-78 Cisco NAC Agent—preference.plist File Contents



RADIUS Challenge-Response Mac OS X Cisco NAC Agent Dialogs

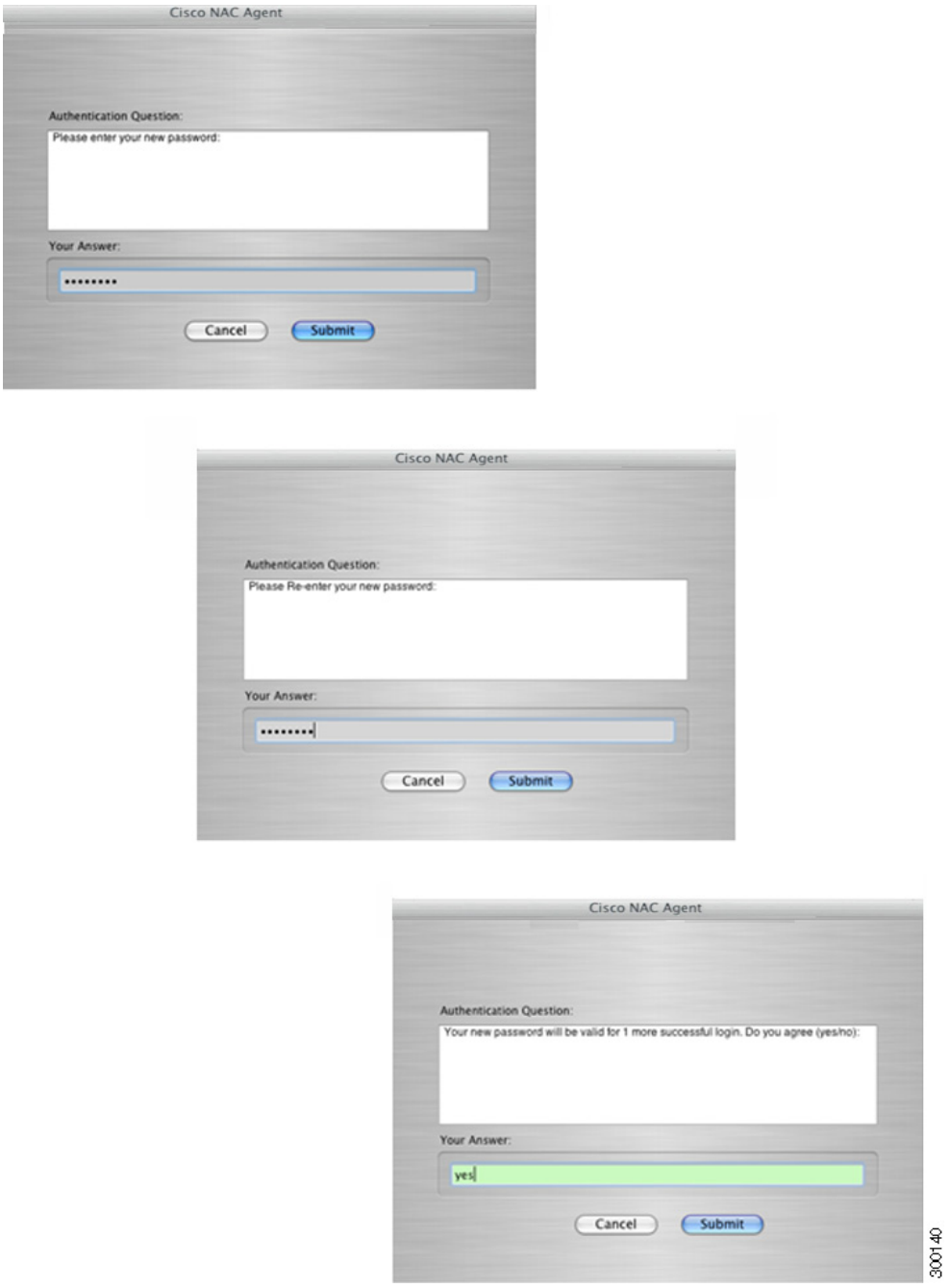
If you configure the Clean Access Manager to use a RADIUS server to validate remote users, the end-user Cisco NAC Agent login session may feature extra authentication challenge-response dialogs not available in other dialog sessions—beyond the standard user ID and password. This additional interaction is due to the user authentication profile on the RADIUS server, itself, and does not require any additional configuration on the Clean Access Manager. For example, the RADIUS server profile configuration may feature an additional authentication challenge like verifying a token-generated PIN or other user-specific credentials in addition to the standard user ID and password. In this case, one or more additional login dialog screens may appear as part of the login session.

The following section provides an example of the dialog exchange for Mac OS X Cisco NAC Agent user authentication.

1. The remote user logs in normally and provides their username and password in the Mac OS X Cisco NAC Agent login dialog.

2. If the associated RADIUS server has been configured to authenticate users with additional credentials, the user is presented with one or more additional challenge-response dialogs (like the password renewal scenario shown in Figure 10-79) for which they must provide additional credentials to authenticate and connect.

Figure 10-79 Additional Mac OS X RADIUS Challenge-Response Dialogs



3. Once the additional challenge-response(s) are validated, the RADIUS server notifies the Clean Access Manager that the user has successfully authenticated and should be granted remote access.



Monitoring and Troubleshooting Agent Sessions

This chapter provides information on compiling and accessing various Cisco NAC Appliance Agent reports and log files and troubleshooting Agent connection and operation issues:

- Viewing Agent Reports, page 11-1
- Create Agent Log Files Using the Cisco Log Packager, page 11-6
- Manage Certified Devices, page 11-10
- Report Settings, page 11-18
- Online Users list, page 11-28
- Agent Troubleshooting, page 11-36

Viewing Agent Reports

The administrator Agent **Reports** page (under **Device Management > Clean Access > Clean Access Agent > Reports > Report Viewer**) gives you detailed information about user Agent sessions. The information includes user access attempts and system check results.

Using the **Reports** page, administrators can log and search Agent reports to facilitate information gathering and export compiled report data to aid statistical analysis and Agent connection issue troubleshooting. The **Reports** page presents Agent report entry information using the following column headings:

Status—Green or red flag indicates successful or unsuccessful Agent connection

User—The user ID used to establish the session from the client machine

Agent—Specifies the type of Cisco NAC Appliance Agent used to initiate the client session

Type—Specifies whether the report has been generated due to Login posture or Passive Re-assessment

IP—The client machine IP address

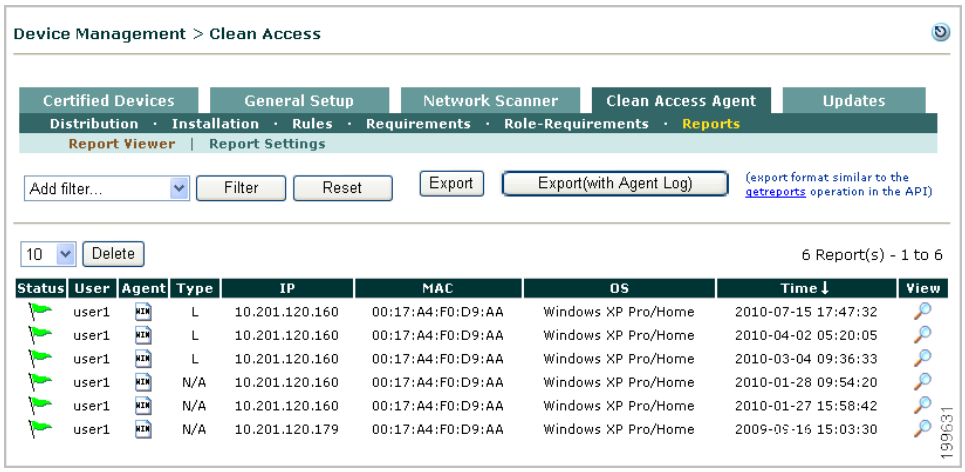
MAC—The client machine interface MAC address

OS—The operating system detected on the client machine

Time—The date and time the user attempted to initiate the Agent session

Note Report List entries with a red background indicate clients who failed system checking.

Figure 11-1 Agent Administrator Report


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Distribution · Installation · Rules · Requirements · Role-Requirements · Reports
Report Viewer | Report Settings
Add filter...
Filter
Reset
Export
Export(with Agent Log)
(export format similar to the getreports operation in the API)
10
Delete
6 Report(s) - 1 to 6
Status User Agent Type IP MAC OS Time View
user1 L 10.201.120.160 00:17:A4:F0:D9:AA Windows XP Pro/Home 2010-07-15 17:47:32
user1 L 10.201.120.160 00:17:A4:F0:D9:AA Windows XP Pro/Home 2010-04-02 05:20:05
user1 L 10.201.120.160 00:17:A4:F0:D9:AA Windows XP Pro/Home 2010-03-04 09:36:33
user1 N/A 10.201.120.160 00:17:A4:F0:D9:AA Windows XP Pro/Home 2010-01-28 09:54:20
user1 N/A 10.201.120.160 00:17:A4:F0:D9:AA Windows XP Pro/Home 2010-01-27 15:58:42
user1 N/A 10.201.120.179 00:17:A4:F0:D9:AA Windows XP Pro/Home 2009-09-16 15:03:30
199631

The Reports page also enables you to filter the list of user session reports by activating and defining additional client report display criteria. For example, if you have a very large user access base where users log in every day (even multiple times per day) and you want to limit the number of reports to a more manageable total, you can choose to display user session information for a single user ID or all user sessions from a specific device. The filter parameters available in the dropdown menu are:

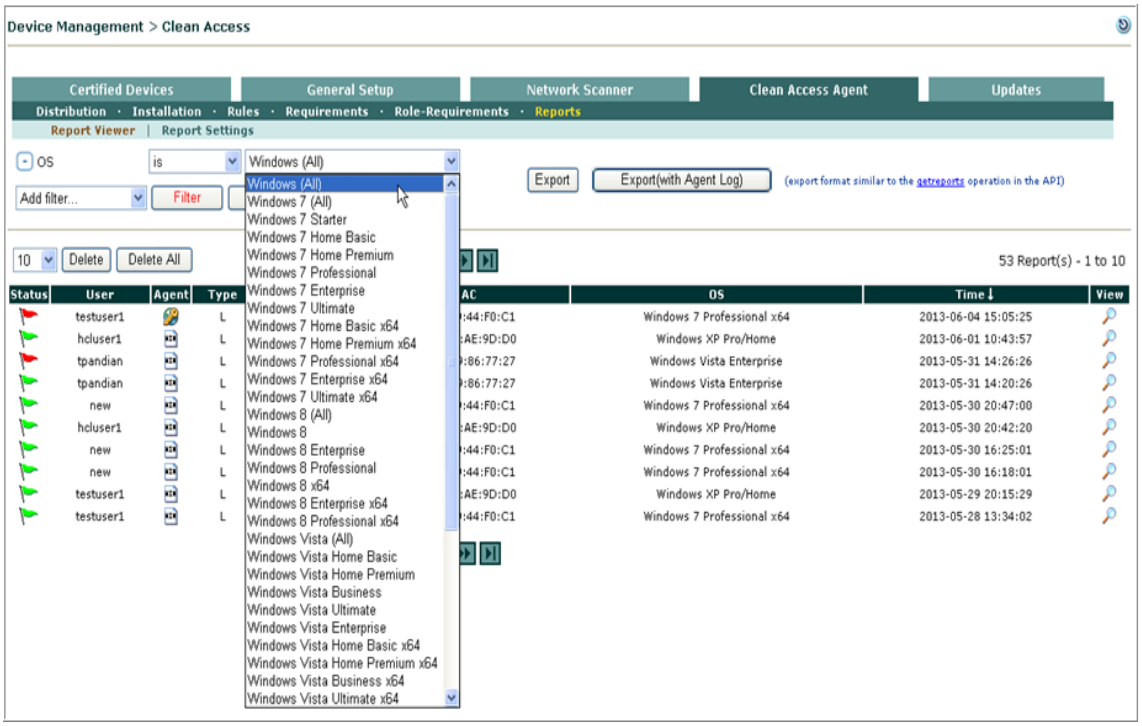
- **Status**—Allows you to list either successful or unsuccessful, or both types of user sessions
- **Username**—Allows you to specify all or part of a specific user ID to display in the client report list
- **Agent**—Allows you to select the type of Cisco NAC Appliance Agent
- **Type**—Allows you select the type of the posture by which the client has got access to the NAC Appliance (Login or Passive Re-assessment)
- **IP**—Allows you to limit the list of client reports to match all or part of a specified IP address (you could use this parameter to limit the user list to only IP addresses in the 10.12.4.<*x*> range by specifying “starts with” “10.12.4.”, for example)
- **MAC**—Allows you to limit the list of client reports to match all or part of a specified source MAC address
- **OS**—Allows you to display client reports based on the operating system detected on the client machine
- **Time**—Allows you to display client report entries either since or before a point in time (like within the last hour or before the last day, for example)
- **Software**—Allows you to display client reports for specific installed AntiVirus, Antispyware, and/or any Unsupported AV/AS software
- **Requirement**—Allows you to display only client reports associated with a specific Agent requirement
- **Requirement Status**—Allows you to display client reports for successful or unsuccessful Agent requirements for the specified **Requirement** (above)
- **System Name**—Allows you to display client reports associated with all or part of a specific client system name
- **System User**—Allows you to display client reports associated with a specific system user (that is, the user logged in to the client machine at the time the actual user session was initiated, which is not necessarily the same ID as the **Username**, above)

- **System Domain**—Allows you to display only client reports based on the system domain into which the client machine has been logged in
- **User Domain**—Allows you to display only client reports based on the user domain with which client **System User** ID is associated

Click the **Filter** button after selecting and defining parameters for any of the search options to display a summary of all client report entries that match the criteria as well as the detailed administrator report for each client.

For example, you can use the **OS** filter option to refine the Agent report display to a smaller number of report entries by selecting one of the options form the dropdown list (Figure 11-2).

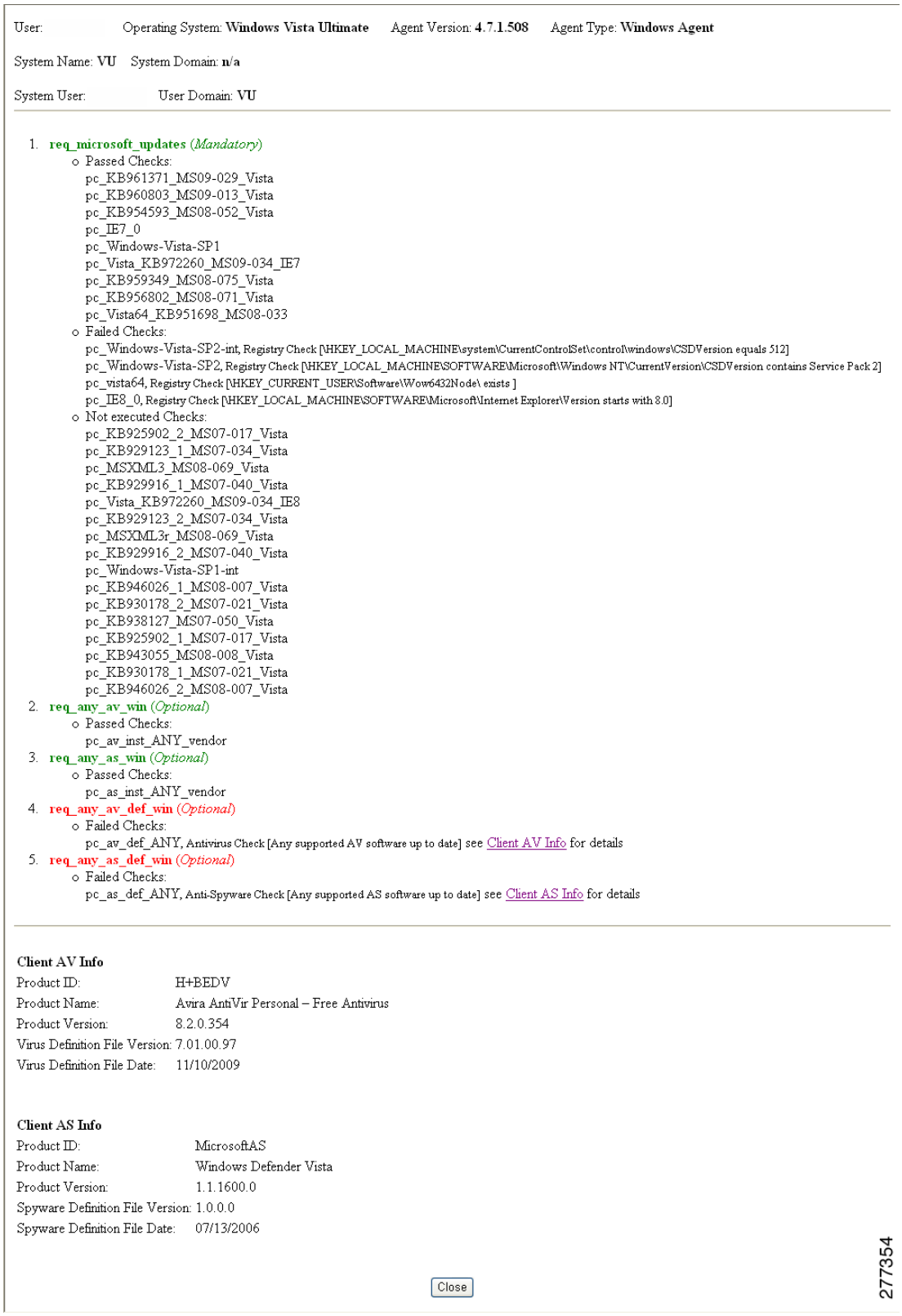
Figure 11-2 Agent Administrator Report—OS Filter Option



You can click **Reset** to negate any of the optional search criteria from the filter dropdown menu and return the client report display list to default settings.

Click the **View** icon (far-right magnifying glass icon) to see an individual user report, as shown in Figure 11-3.

Figure 11-3 Example Agent Report



User: Operating System: **Windows Vista Ultimate** Agent Version: **4.7.1.508** Agent Type: **Windows Agent**

System Name: **VU** System Domain: **n/a**

System User: User Domain: **VU**

1. **req_microsoft_updates** (*Mandatory*)
   - Passed Checks:
     pc_KB961371_MS09-029_Vista
     pc_KB960803_MS09-013_Vista
     pc_KB954593_MS08-052_Vista
     pc_IE7_0
     pc_Windows-Vista-SP1
     pc_Vista_KB972260_MS09-034_IE7
     pc_KB959349_MS08-075_Vista
     pc_KB956802_MS08-071_Vista
     pc_Vista64_KB951698_MS08-033
   - Failed Checks:
     pc_Windows-Vista-SP2-int, Registry Check [HKEY_LOCAL_MACHINE\system\CurrentControlSet\control\windows\CSDVersion equals 512]
     pc_Windows-Vista-SP2, Registry Check [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion contains Service Pack 2]
     pc_vista64, Registry Check [HKEY_CURRENT_USER\Software\Wow6432Node\ exists]
     pc_IE8_0, Registry Check [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version starts with 8.0]
   - Not executed Checks:
     pc_KB925902_2_MS07-017_Vista
     pc_KB929123_1_MS07-034_Vista
     pc_MSXML3_MS08-069_Vista
     pc_KB929916_1_MS07-040_Vista
     pc_Vista_KB972260_MS09-034_IE8
     pc_KB929123_2_MS07-034_Vista
     pc_MSXML3r_MS08-069_Vista
     pc_KB929916_2_MS07-040_Vista
     pc_Windows-Vista-SP1-int
     pc_KB946026_1_MS08-007_Vista
     pc_KB930178_2_MS07-021_Vista
     pc_KB938127_MS07-050_Vista
     pc_KB925902_1_MS07-017_Vista
     pc_KB943055_MS08-008_Vista
     pc_KB930178_1_MS07-021_Vista
     pc_KB946026_2_MS08-007_Vista
2. **req_any_av_win** (*Optional*)
   - Passed Checks:
     pc_av_inst_ANY_vendor
3. **req_any_as_win** (*Optional*)
   - Passed Checks:
     pc_as_inst_ANY_vendor
4. **req_any_av_def_win** (*Optional*)
   - Failed Checks:
     pc_av_def_ANY, Antivirus Check [Any supported AV software up to date] see Client AV Info for details
5. **req_any_as_def_win** (*Optional*)
   - Failed Checks:
     pc_as_def_ANY, Anti-Spyware Check [Any supported AS software up to date] see Client AS Info for details

Client AV Info

Product ID: H+BEDV
Product Name: Avira AntiVir Personal – Free Antivirus
Product Version: 8.2.0.354
Virus Definition File Version: 7.01.00.97
Virus Definition File Date: 11/10/2009

Client AS Info

Product ID: MicrosoftAS
Product Name: Windows Defender Vista
Product Version: 1.1.1600.0
Spyware Definition File Version: 1.0.0.0
Spyware Definition File Date: 07/13/2006

Close

277354

In addition to user, operating system, Agent version, and domain information, the Agent report lists the requirements applicable for the user role (both mandatory and optional). Requirements that the user met are listed in green, and failed requirements are listed in red. The individual checks making up the requirement are listed by status of Passed, Failed, or Not executed. This allows you to view exactly which check a user failed when a requirement was not met.

Not Executed checks are checks that were not applied, for example because they apply to a different operating system. **Failed** checks may be the result of an "OR" operation. To clear the reports, click the **Delete** button. The button clears all the report entries that are currently selected by the filtering criteria.

Exporting Agent Reports

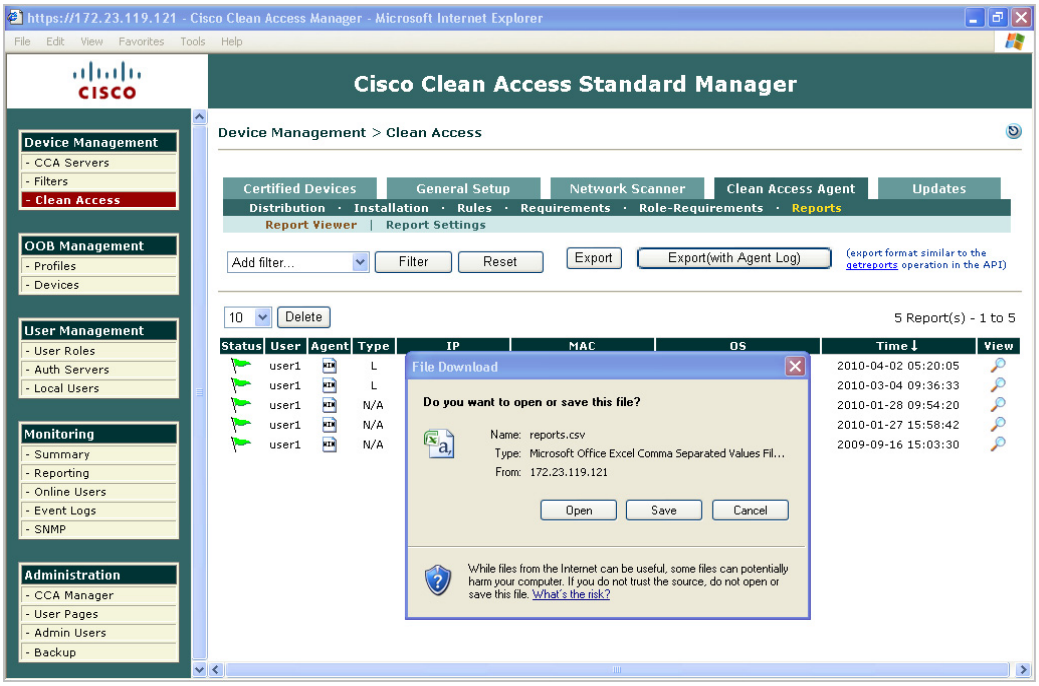
You can use the **Export** and **Export (with text)** buttons to save CSV files containing Agent report data to your local hard drive to search, view, and manipulate whenever needed for troubleshooting or statistical analysis purposes.

Step 1 Go to under **Device Management > Clean Access > Clean Access Agent > Reports > Report Viewer** (see Figure 11-4).

Step 2 Click **Export** or **Export (with text)**.

Note Due to limits native to the Microsoft Excel application, you can only export up to 65534 entries using this function.

Figure 11-4 Exporting Agent Reports



Step 3 Do one of the following:

- Click **Open** to view the resulting Agent report file.

- Click **Save**, navigate to a directory on your local machine where you want to save the Agent report file, enter a name for the file, and click **Save** in the navigation dialog so you can view the report at a later date.

Limiting the Number of Reports

You can limit the number of reports in the log under **Device Management > Clean Access > Clean Access Agent > Reports > Report Setting**. Specify the maximum number of reports as a value between 100 and 200000 (default is 30000).

Agent reports are stored in their own table and are separate from the general Event Logs.

Create Agent Log Files Using the Cisco Log Packager

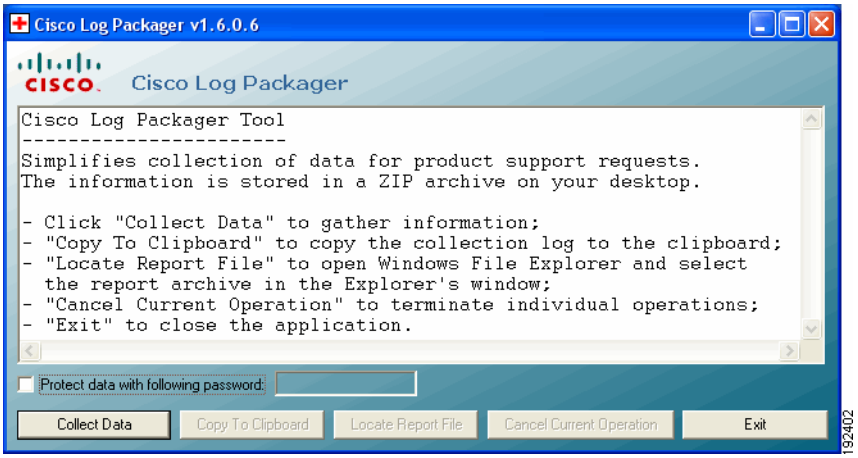
When users download the Cisco NAC Agent, the installation process also adds the Cisco Log Packager utility to the client machine in the same relative Program File location as Agent files. The Log Packager utility compiles and saves a number of different types of Agent logs in a single .zip file (named **CiscoSupportReport.zip**) and saves it on the client machine's desktop, so the user can access the information easily and forward on to network administrators to help troubleshoot Agent session login and/or operation issues.

Note In Cisco NAC Appliance Release 4.6(1) and later, the Cisco Log Packager application is only available for English and Japanese Windows platforms.

To launch the Cisco Log Packager:

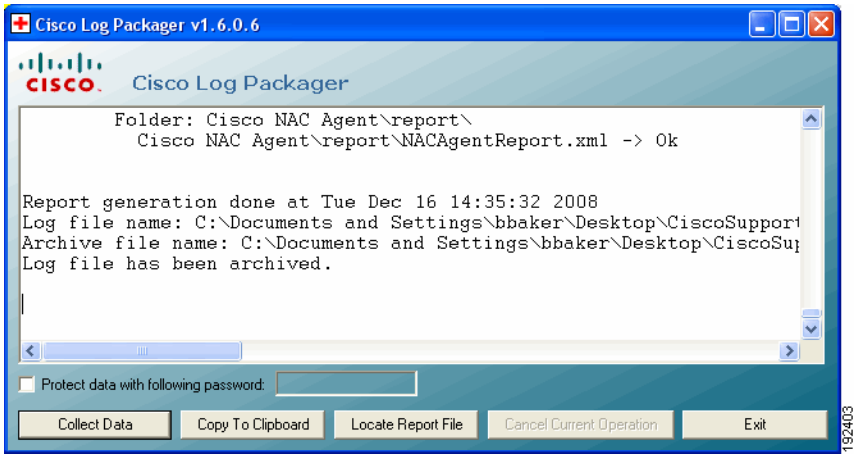
Step 1 On the Windows client machine, navigate to Start > Program Files > Cisco > Client Utilities > Cisco Log Packager (Figure 11-5).

Figure 11-5 Cisco Log Packager


Cisco Log Packager v1.6.0.6
Cisco Log Packager
Cisco Log Packager Tool
Simplifies collection of data for product support requests.
The information is stored in a ZIP archive on your desktop.
- Click "Collect Data" to gather information;
- "Copy To Clipboard" to copy the collection log to the clipboard;
- "Locate Report File" to open Windows File Explorer and select the report archive in the Explorer's window;
- "Cancel Current Operation" to terminate individual operations;
- "Exit" to close the application.
Protect data with following password:
Collect Data
Copy To Clipboard
Locate Report File
Cancel Current Operation
Exit
192402

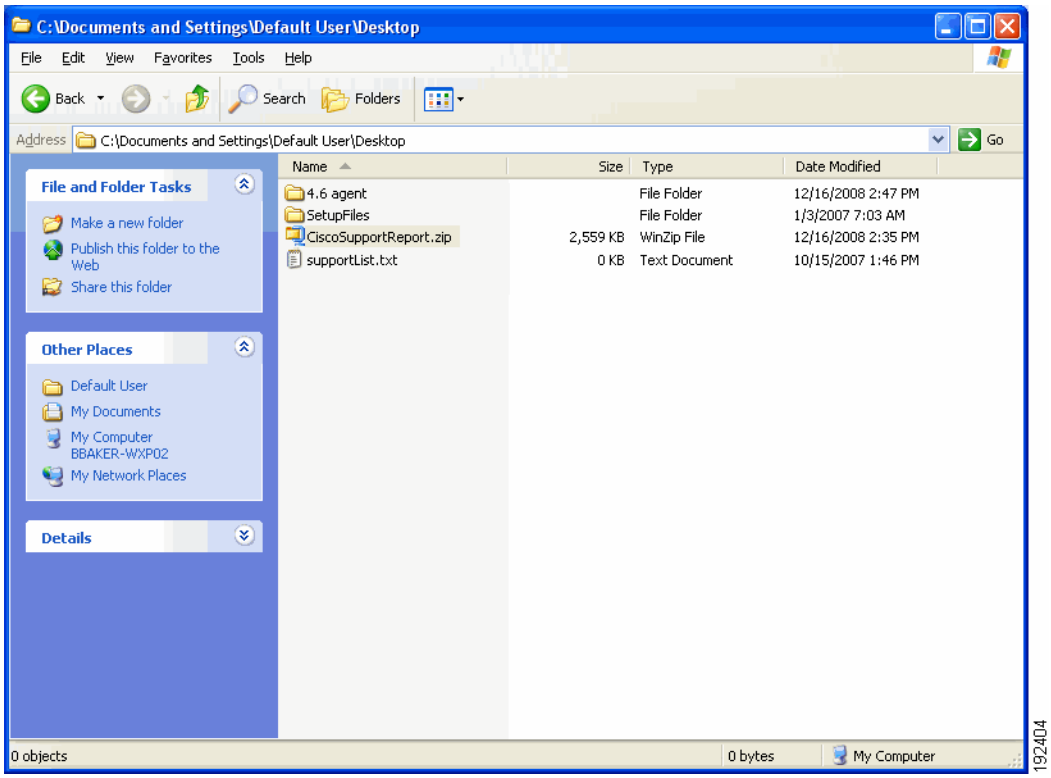
Step 2 Click **Collect Data** and wait for the Cisco Log Packager to complete compiling the Agent log information. This step takes anywhere from several seconds to a couple of minutes or so. The process is complete when you see a "Log file has been archived" message in the Cisco Log Packager display window and the **Copy to Clipboard** and **Locate Log File** buttons become active (Figure 11-6).

Figure 11-6 Cisco Log Packager—Log File Archive Complete


Cisco Log Packager v1.6.0.6
Cisco Log Packager
Folder: Cisco NAC Agent\report\
Cisco NAC Agent\report\NACAgentReport.xml -> Ok
Report generation done at Tue Dec 16 14:35:32 2008
Log file name: C:\Documents and Settings\bbaker\Desktop\CiscoSupport
Archive file name: C:\Documents and Settings\bbaker\Desktop\CiscoSu
Log file has been archived.
Protect data with following password:
Collect Data
Copy To Clipboard
Locate Report File
Cancel Current Operation
Exit
192403

Step 3 To automatically navigate to the location on the client machine where the log file has been compiled and saved, click **Locate Log File**. A Windows Explorer dialog box opens highlighting the location of the new **CiscoSupprtReport.zip** log file on the client machine desktop (Figure 11-7).

Figure 11-7 Agent Log File Location



Use the **CiscoSupprtReport.zip** log file to help diagnose and troubleshoot Agent login/operation issues. Users can send the .zip file to their respective Cisco NAC Appliance system administrator or, if performing local troubleshooting, extract and view the contents of the various Cisco Log Packager files on the client machine. For details on the files included in the **CiscoSupprtReport.zip** log file and their purpose, see Figure 11-7.

Table 11-1 Cisco Log Packager Files

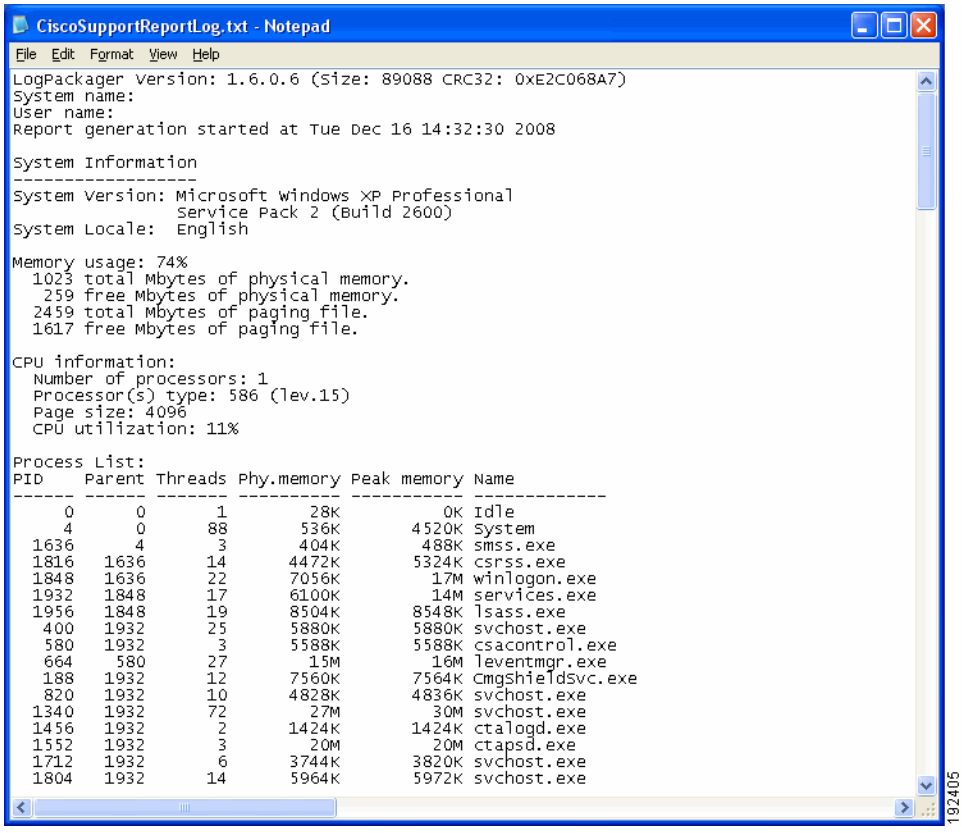
Agent Log File Name	Contents/Description
CiscoSupportReportLog.txt	This text file contains client machine system information, including CPU usage and memory allocation.
ipinfo.log	This log file contains network configuration and network connection status, including client machine IP interface status, IP statistics, and the client ARP table.
NACAgentLogPlugin.log	This user-inaccessible log is one of the modules in the LogPacker component that calls the NACAgentDiags function to generate the NACAgentDiagnosticLog.txt log report.
NACAgentDiagnosticsLog.txt	This user-inaccessible text file contains diagnostic messages used to help debug AV issues.
NACAgentDiagsLogMessages.txt	This text file contains other regular log messages not used in the diagnostics output.
NACAgentLogCurrent.log	This is an encrypted log file that contains the current Cisco NAC Agent messages from the active session and is used primarily to help debug Cisco NAC Agent issues. When the system reboots or services have been restarted, the existing **NACAgentLogOld.log** is erased, the active **NACAgentLogCurrent.log** becomes the new **NACAgentLogOld.log**, and a new **NACAgentLogCurrent.log** is created. **Note** You can configure the size of Agent log files using the **LogFileSize** parameter in the **NACAgentCFG.xml** Agent configuration XML file. If set to 0, no logging takes place. If set to non-zero, then the log file does not grow larger than the value (in Megabytes). The default is 5 MB. When **NACAgentLogCurrent.log** reaches the setting value, it is copied to **NACAgentLogOld.log** and a new **NACAgentLogCurrent.log** is created.

Table 11-1 Cisco Log Packager Files

Agent Log File Name	Contents/Description
NACAgentLogOld.log	This is an encrypted log file that contains output from the previous active Cisco NAC Agent session and is also used to help debug Cisco NAC Agent issues. This file is created in one of two ways: • The "archived" log file from an active Cisco NAC Agent session that reached its maximum size (configured using the **LogFileSize** parameter in the **NACAgentCFG.xml** Agent configuration XML file). • When the system reboots or services are restarted, the existing **NACAgentLogOld.log** is erased, the active **NACAgentLogCurrent.log** becomes the new **NACAgentLogOld.log**, and a new **NACAgentLogCurrent.log** is created.

Users can open any of the .txt files on the client machine using a standard text editor application and view the report contents. Figure 11-8 shows the contents of a **CiscoSupportReportLog.txt** file opened using Microsoft Notepad on the client machine.

Figure 11-8 CiscoSupportReportLog.txt File Contents


CiscoSupportReportLog.txt - Notepad
File Edit Format View Help
LogPackager Version: 1.6.0.6 (Size: 89088 CRC32: 0xE2C068A7)
System name:
User name:
Report generation started at Tue Dec 16 14:32:30 2008
System Information
System Version: Microsoft Windows XP Professional
Service Pack 2 (Build 2600)
System Locale: English
Memory usage: 74%
1023 total Mbytes of physical memory.
259 free Mbytes of physical memory.
2459 total Mbytes of paging file.
1617 free Mbytes of paging file.
CPU information:
Number of processors: 1
Processor(s) type: 586 (lev.15)
Page size: 4096
CPU utilization: 11%
Process List:
PID Parent Threads Phy.memory Peak memory Name
0 0 1 28K 0K Idle
4 0 88 536K 4520K System
1636 4 3 404K 488K smss.exe
1816 1636 14 4472K 5324K csrss.exe
1848 1636 22 7056K 17M winlogon.exe
1932 1848 17 6100K 14M services.exe
1956 1848 19 8504K 8548K lsass.exe
400 1932 25 5880K 5880K svchost.exe
580 1932 3 5588K 5588K csacontrol.exe
664 580 27 15M 16M leventmgr.exe
188 1932 12 7560K 7564K CmgShieldSvc.exe
820 1932 10 4828K 4836K svchost.exe
1340 1932 72 27M 30M svchost.exe
1456 1932 2 1424K 1424K ctalogd.exe
1552 1932 3 20M 20M ctapsd.exe
1712 1932 6 3744K 3820K svchost.exe
1804 1932 14 5964K 5972K svchost.exe
192405

Manage Certified Devices

This section describes the following:

- Add Exempt Device, page 11-12
- Clear Certified or Exempt Devices Manually, page 11-13
- View Reports for Certified Devices, page 11-13
- View Switch/WLC Information for Out-of-Band Certified Devices, page 11-13
- Configure Certified Device Timer, page 11-14
- Add Floating Devices, page 11-16

The Clean Access Manager web console provides two important lists that manage users and their devices: the **Online Users** list (both In-Band and Out-of-Band) and **Certified Devices List**. The Online Users list displays logged-in users by IP address and login credentials (see Interpreting Event Logs, page 13-4). When a user device passes network scanning or meets Agent Requirements, the Clean Access Server automatically adds the MAC address of the device to the Certified Devices List (for users with Layer 2 proximity to the CAS).

Note Because the Certified Devices List is based on client MAC addresses, the Certified Devices List never applies to users in Layer 3 deployments. Web login users that are one or more Layer 3 hops away from the CAS are tracked by IP address only, unless the ActiveX/Java applet web client is enabled for the login page (to obtain the MAC address of the client). For further details on Layer 3 deployment, see "Enable L3 Deployment Support" in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Dropping an In-Band user from the In-Band Online Users list does not remove the client device from the Certified Devices List. However, manually dropping an In-Band client from the Certified Devices List automatically removes the user from the network and the In-Band Online Users list.

Dropping an Out-of-Band user from the Out-of-Band Online Users list has different results depending on your Cisco NAC Appliance configuration:

- In a deployment where Out-of-Band Logoff has been enabled, the client machine is also automatically removed from the Certified Devices List.
- If Out-of-Band Logoff is not enabled and you kick the user from the Out-of-Band Online Users list, the client machine stays in the Certified Devices List just as with an In-Band deployment.

  For more information on Out-of-Band logoff, see Configure Out-of-Band Logoff, page 9-6.

For network scanning, once on the Certified Devices List, the device does not have to be recertified as long as its MAC address is in the Certified Devices List, even if the user of the device logs out and accesses the network again as another user. Dropping a client from the Certified Devices List forces the user to repeat authentication and the device to repeat network scanning to be readmitted to the network. (Multi-user devices should be configured as floating devices to require recertification at each login.) You can make sure that a device is always removed from the Certified Devices List when a network scanning user logs off by enabling the option **Require users to be certified at every web login** in the **General Setup > Web Login** tab (see Client Login Overview, page 1-6.)

For Agent users, devices always go through Agent Requirements at each login, even if the device is already on the Certified Devices List. In addition, the Certified Devices List only records the first user that logged in with the device. This helps to identify the authenticating user who accepted the User

Agreement Page (for web login users) or the Network Policy Page (for Agent users) if either page was configured for the role. See Table 1-2 "Web Login—General Setup Configuration Options" and Table 1-3 "Web Login User Page Summary" for details on these pages.

A certified device remains on the Certified Devices List until:

- The list is automatically cleared using a Certified Devices Timer.
- The administrator manually clears the entire list.
- The administrator manually drops the client from the list.
- The user logs out or is removed from the network, and the **Require users to be certified at every web login** option is checked for the role from the **General Setup > Web Login** page.

Devices automatically added to the Certified Devices List can be cleared manually or cleared automatically at specified intervals. Because the administrator must manually add exempt devices to the list, the administrator must also manually remove them. This means that an exempt device on the Certified Devices List is protected from being automatically removed when the global Certified Devices Timer form is used to clear the list at regularly scheduled intervals.

Clearing devices from the Certified Devices List (whether manually or automatically) performs the following actions:

- Removes IB clients from the In-Band Online Users list and logs them off the network.
- Removes OOB clients from the Out-of-Band Online Users list and bounces their port (unless port bouncing is disabled for OOB VGW; see Add Port Profile, page 3-34 for details).
- Forces client devices to repeat posture assessment at the next login.

Once off the Certified Devices List, the client must pass network scanning and meet Agent Requirements again to be readmitted to the network. You can add floating devices that are certified only for the duration of a user session. You can also exempt network scanning devices from Nessus Scanning altogether by manually adding them to the Certified Devices List.

If using a Certified Device timer, you can configure whether or not a user is removed when the list is cleared by enabling/disabling the **Keep Online Users** option for the timer. See Configure Certified Device Timer, page 11-14 for further details.

Note that logging an IB user off the network from **Monitoring > Online Users > View Online Users** does not remove the client from the Certified Devices List. This allows the user to log in again without forcing the client machine to go through posture assessment again. Note that for Agent users, devices always go through Agent Requirements at each login, even if the device is already on the Certified Devices List.



Note Because the Certified Devices List displays users authenticated and certified based on known L2 MAC address, the Certified Devices List does not display information for remote VPN/multihop L3 users tracked by IP address only. To view these authenticated remote VPN/multihop L3 users, see the In-Band Online Users list. The User MAC field for these user entries appears as "00:00:00:00:00:00."

For further details on terminating active user sessions, see Interpreting Active Users, page 11-29 and Out-of-Band Users, page 3-68.

If a certified device is moved from one CAS to another, it must go through Nessus Scanning again for the new CAS unless it has been manually added as an exempt device at the global level for all Clean Access Servers. This allows for the case where one Clean Access Server has more restrictive posture assessment requirements than another.

Though devices can only be certified and added to the list per Clean Access Server, you can remove certified devices globally from all Clean Access Servers or locally from a particular CAS only (see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for additional details.) For additional information, see also Out-of-Band Users, page 3-68.

Add Exempt Device

Designating a device as **Exempt** excludes the device from Network Scanning (Nessus scans) and no network scanning report is generated for the client. Exempting a device manually adds it the to Certified Devices List and allows it to bypass network scanning as long as its MAC address remains on the list.

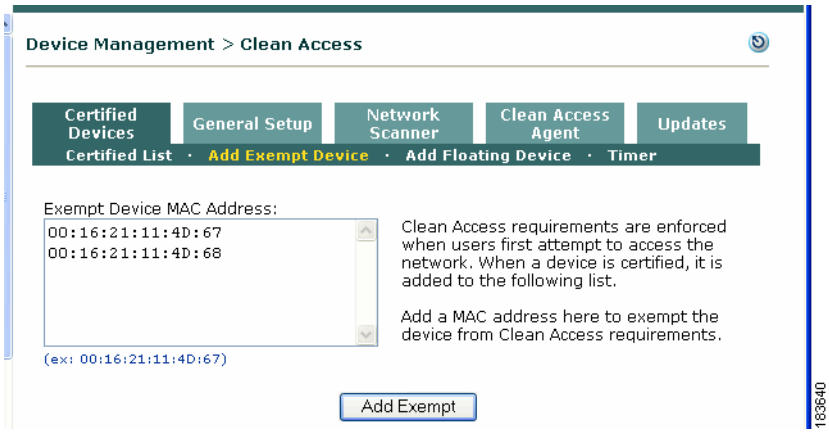
Note Adding a device as Exempt does not exempt the client machine from Agent posture assessment.

Note For details on how to allow users/devices to bypass authentication, see Global Device and Subnet Filtering, page 2-10.

To add an exempt device:

Step 1 Go to **Device Management > Clean Access > Certified Devices > Add Exempt Device**.

Figure 11-9 Add Exempt Device


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Certified List · Add Exempt Device · Add Floating Device · Timer
Exempt Device MAC Address:
00:16:21:11:4D:67
00:16:21:11:4D:68
(ex: 00:16:21:11:4D:67)
Clean Access requirements are enforced when users first attempt to access the network. When a device is certified, it is added to the following list.
Add a MAC address here to exempt the device from Clean Access requirements.
Add Exempt
183640

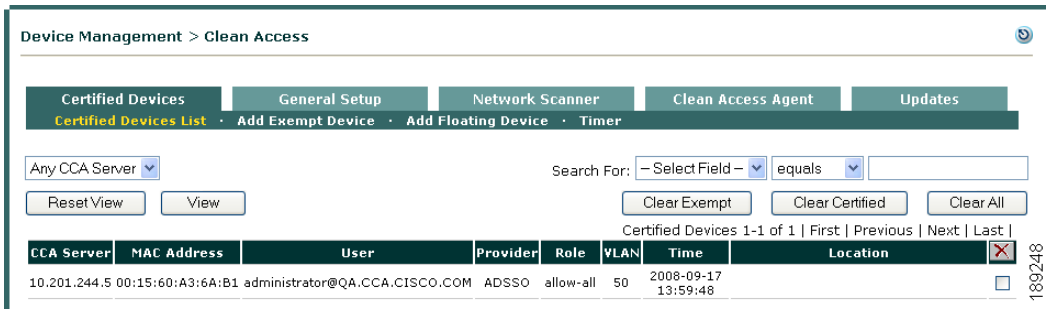
Step 2 Type the MAC address in the **Exempt Device MAC Address** field. To add several addresses at once, use line breaks to separate the addresses.

Step 3 Click **Add Exempt**.

Step 4 The **Certified Devices List** page appears, highlighting the exempt devices (Figure 11-10).

Note Exempt devices added with these forms are exempt for all Clean Access Servers. To designate an exempt device for only a particular Clean Access Server, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Figure 11-10 Clean Access Certified Devices List



Clear Certified or Exempt Devices Manually

To clear device MAC addresses, go to **Device Management > Clean Access > Certified Devices > Certified Devices List** and click:

- **Clear Exempt** to remove only the MAC addresses that were added manually with the **Add Exempt** button.
- **Clear Certified** to remove only the MAC addresses that were added automatically by the Clean Access Server.
- **Clear All** to remove MAC addresses of both exempt and certified devices.

Remove individual addresses individually by clicking **Delete** next to the MAC address.

View Reports for Certified Devices

You can view the results of previous Agent scans for certified devices under **Device Management > Clean Access > Clean Access Agent > Reports.** Click the **View** icon to see which requirements, rules, and checks succeeded or failed for an individual client. See View Scan Reports, page 12-17 for details.

You can view the results of previous network scans for certified devices at any time from **Device Management > Clean Access > Network Scanner > Reports.** Click the **Report** icon to see an individual scan report. See View Scan Reports, page 12-17 for details.

View Switch/WLC Information for Out-of-Band Certified Devices

For Out-of-Band users only, the **Certified Devices List** (Figure 11-10) populates the **Location** column with a the IP address and specific port on the Out-of-Band switch, or (in the case of a Wireless LAN controller) the IP address and SSID for the specific Out-of-Band WLC.

For further details on OOB clients, see:

- Chapter 3, “Switch Management: Configuring Out-of-Band Deployment” and Out-of-Band Users, page 11-31
- Chapter 4, “Wireless LAN Controller Management: Configuring Wireless Out-of-Band Deployment”

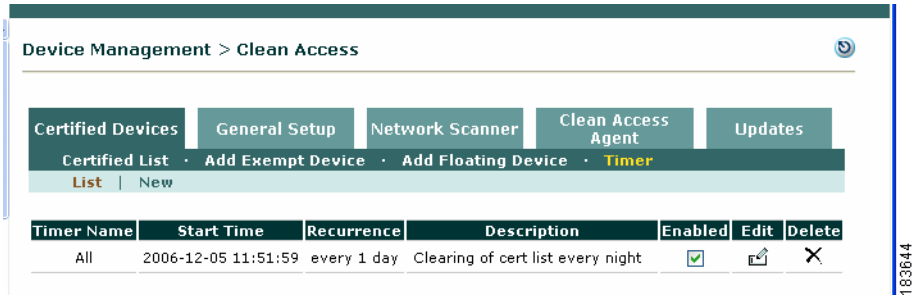
Configure Certified Device Timer

You can configure Certified Device **Timer**s to automatically clear the Certified Device list at specified intervals. The Certified Devices List no longer needs to be cleared in its entirety each time the timer is applied. Administrators can now:

- Clear the Certified Devices List per Clean Access Server, User Role, or Authentication Provider, or a combination of all three.
- Clear certified devices without removing users from the network with the "Keep Online Users" option. When the "Keep Online Users" option is checked, user sessions are not immediately ended when clearing the list, but at user logout time (or at linkdown for OOB). Devices can re-enter the list after user authentication and device remediation.
- Clear the Certified Devices List all at once or in batches (to manage user re-login and certification during peak times). You can clear devices according to how long they have been on the list and/or in fixed time interval batches. This facilitates CAM database management when clearing large numbers of devices.
- Configure multiple independent timers. Administrators can create and save multiple instances of Certified Device Timers (similar to a Scheduled Job/Task). Each Timer is independent of the others and can be maintained separately. For example, if managing 6 CAS pairs, the administrator can create a different Timer for each pair of HA-CASs.

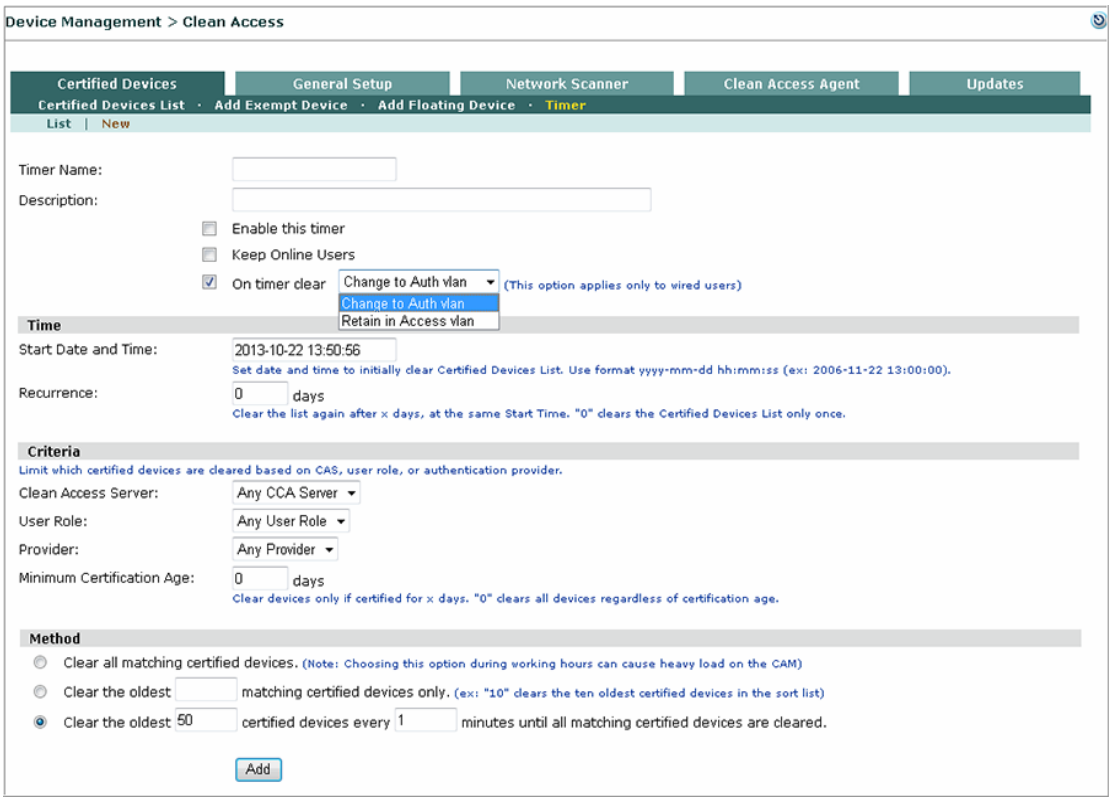
Step 1 Go to **Device Management > Clean Access > Certified Devices > Timer**. The **List** page appears by default.

Figure 11-11 Certified Devices Timer—List



Step 2 Click the **New** sublink to bring up the **New Timer** configuration form.

Figure 11-12 New Certified Devices Timer


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Certified Devices List · Add Exempt Device · Add Floating Device · Timer
List | New
Timer Name:
Description:
Enable this timer
Keep Online Users
On timer clear
Change to Auth vlan
(This option applies only to wired users)
Change to Auth vlan
Retain in Access vlan
Time
Start Date and Time:
2013-10-22 13:50:56
Set date and time to initially clear Certified Devices List. Use format yyyy-mm-dd hh:mm:ss (ex: 2006-11-22 13:00:00).
Recurrence:
0
days
Clear the list again after x days, at the same Start Time. "0" clears the Certified Devices List only once.
Criteria
Limit which certified devices are cleared based on CAS, user role, or authentication provider.
Clean Access Server:
Any CCA Server
User Role:
Any User Role
Provider:
Any Provider
Minimum Certification Age:
0
days
Clear devices only if certified for x days. "0" clears all devices regardless of certification age.
Method
Clear all matching certified devices. (Note: Choosing this option during working hours can cause heavy load on the CAM)
Clear the oldest
matching certified devices only. (ex: "10" clears the ten oldest certified devices in the sort list)
Clear the oldest 50 certified devices every 1 minutes until all matching certified devices are cleared.
Add
370763

Step 3 Type a **Timer Name** for the timer.

Step 4 Type an optional **Description** of the timer.

Step 5 Click the checkbox for **Enable this timer** to apply the timer right away after configuration.

Step 6 Click the checkbox for **Keep Online Users** if you only want to remove client devices from the Certified Devices List without removing the users from the network.

Step 7 Click the checkbox **On timer clear** to set the users to remain in Access VLAN or move to Auth VLAN. From the drop-down, choose **Retain in Access vlan** to remove the users from CDL and remain in Access VLAN. You can choose **Change to Auth vlan** to remove the users from CDL and to move the users to Auth VLAN. This option is available starting from Cisco NAC Appliance Release 4.9(3).

Step 8 Type the **Start Date and Time** for the timer, using format: **YYYY-MM-DD hh:mm:ss**. The **Start Date and Time** sets the initial date and time for this timer to clear the Certified Devices List.

Step 9 Type a **Recurrence** in days to set the repeat interval for this timer. For example, a **Recurrence** of 7 will clear the Certified Devices List 7 days after the initial clearing and at the same **Start Time** specified. Typing **0** will clear the Certified Devices List only once.

Step 10 Choose from any of the dropdown menus to apply this timer by the following **Criteria**:

a. **Clean Access Server**: Apply this timer to **Any CCA Server** (default) or to a specific CAS by IP address.

b. **User Role**: Apply this timer to **Any User Role** (default) or to a specific system user role

c. **Provider**: Apply this timer to **Any Provider** (default) or to a specific system **Auth Provider** (Local DB or any other)

Step 11 Type a **Minimum Age** in days to only clear devices that have been on the Certified Devices List for the number of days specified. Typing **0** clears all devices regardless of how long they have been on the Certified Devices List.

Step 12 Choose a clearing **Method** for how much of the Certified Devices List (sorted by Criteria) this timer should clear at one time. Options are:

a. **Clear all matching certified devices**.

b. **Clear the oldest [] matching certified devices only**. (for example, "10" clears the ten oldest certified devices in the sort list)

c. **Clear the oldest [] certified devices every [] minutes until all matching certified devices are cleared**.

Step 13 When done, click **Update**. This saves the Timer in the Certified Devices Timer List.

Note For additional information on terminating user sessions, see also Configure User Session and Heartbeat Timeouts, page 8-15.

Add Floating Devices

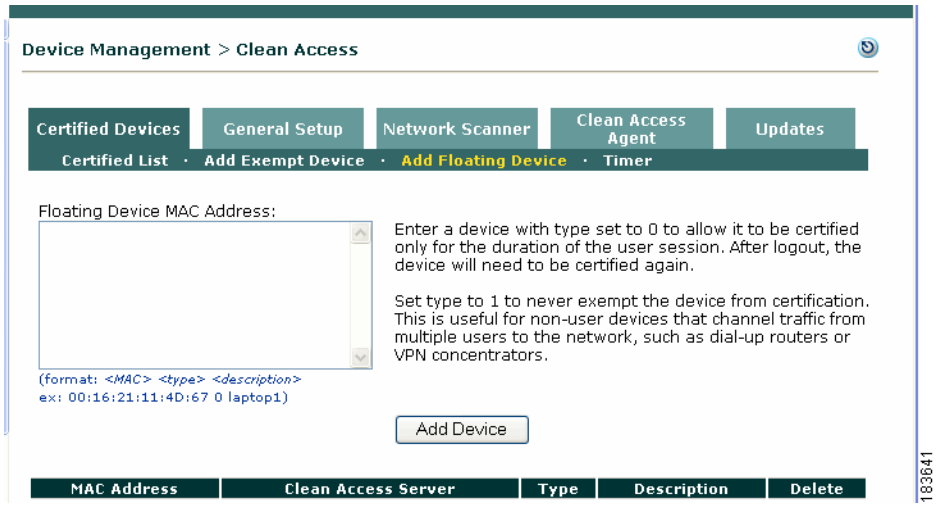
A floating device is certified only for the duration of a user session. Once the user logs out, the next user of the device needs to be certified again. Floating devices are useful for managing shared equipment, such as kiosk computers or wireless cards loaned out by a library.

In addition to session-length certification, you can configure devices that are never certified. This is useful for multi-user devices, such as dial-up routers that channel multi-user traffic from the untrusted side of the network. In this case, the Clean Access Server will see only that device's MAC address as the source and destination of the network traffic. If the device is allowed to be certified, after the first user is certified, additional users would be exempt from certification. By configuring the router's MAC address as a floating device that is never certified, you can ensure that each user accessing the network through the device is individually assessed for vulnerabilities/requirements met.

In this case, the users are distinguished by IP address. Users must have different IP addresses. If the router performs NATing services, the users are indistinguishable to the Clean Access Manager and only the first user will be certified.

Figure 11-13 shows the **Floating Devices** tab.

Figure 11-13 Floating Devices


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Certified List · Add Exempt Device · Add Floating Device · Timer
Floating Device MAC Address:
Enter a device with type set to 0 to allow it to be certified only for the duration of the user session. After logout, the device will need to be certified again.
Set type to 1 to never exempt the device from certification. This is useful for non-user devices that channel traffic from multiple users to the network, such as dial-up routers or VPN concentrators.
(format: <MAC> <type> <description>
ex: 00:16:21:11:4D:67 0 laptop1)
Add Device
MAC Address
Clean Access Server
Type
Description
Delete
183641

Note For VPN concentrator/multihop L3 deployment, administrators must add the MAC address of the router/VPN concentrator to the Floating Device list (example entry: 00:16:21:11:4D:67 1 vpn_concentrator). See "Integrating with Cisco VPN Concentrators" in the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

To configure a floating device:

1. Go to **Device Management > Clean Access > Certified Devices > Add Floating Device**.
2. In the **Floating Device MAC Address** field, enter the MAC address. Type the entry in the form:

   `<MAC> <type> <description>`

   Where:

   - `<MAC>` is the MAC address of the device.
   - `<type>` is either:

     `0` for session-scope certification, or

     `1` if the device should never be considered certified
   - `<description>` is an optional description of the device.

   Include spaces between each element and use line breaks to separate multiple entries. For example:

   ```
   00:16:21:23:4D:67 0 LibCard1
   00:16:34:21:4C:68 0 LibCard2
   00:16:11:12:4A:71 1 Router1
   ```

3. Click **Add Device** to save the setting.

To remove a floating device, click the **Delete** icon for the MAC address.

Report Settings

The **Monitoring > Reporting** tab can be used to enable or disable the reporting and user activity logging, to view the current system information, to customize the reports, and to view the preset reports. This section contains the following topics:

- Dashboard, page 11-18
- Custom Reports, page 11-22
- Configuration, page 11-27

Dashboard

The current system information of the CAM and CAS can be viewed from **Monitoring > Reporting > Dashboard** tab.

The Dashboard page displays the system information, which is constantly monitored and updated. This page is enabled only when the **Enable Dashboard and related tasks** checkbox is checked in the **Monitoring > Reporting > Configuration** page**.**

Note Dashboard and related tasks check box is enabled by default when you upgrade from previous version of NAC release. The default landing page will be the dashboard summary page.

The current system information is displayed as different subtabs in this page. Click the appropriate tabs to view the following information:

- Current Status, page 11-18
- CCA Servers, page 11-20
- Managed Switches, page 11-20
- Authentication Servers, page 11-21
- User Statistics, page 11-22

Current Status

This tab displays the current status of the following:

- **System Summary**: Displays the details of the CAM along with the License details, NAC version installed, NAC Agent versions and so on.
  - Service Uptime: Time since the perfigo service started.
  - Active Uptime: Time since the perfigo service is active on the CAM.
- **Status Summary**: Displays the details of CAM, CAS, OOB Switches, Auth Server and so on.
- **Top 5 CASs:** Displays the CASs with maximum number of current online users in the system.
- **User Summary**: Displays a graphical summary of number of users in online status with reference to time. This graph displays details based on assigned user roles.
- **Recent Events**: Displays system events that happened in the last 5 days.

Note The **Current Status** tab displays the "last refreshed" date and time at the top-right corner of the page. The current system information is automatically refreshed every 10 minutes. You can also refresh the page manually by clicking the **Current Status** tab.

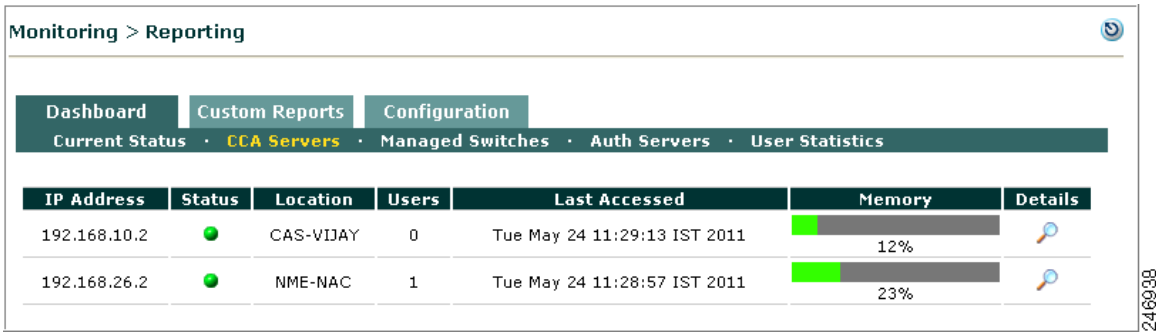
Figure 11-14 Dashboard > Current Status


Monitoring > Reporting
Dashboard
Custom Reports
Configuration
Current Status · CCA Servers · Managed Switches · Auth Servers · User Statistics
Last Refresh: Fri May 20 11:38:23 IST 2011
System Summary
Primary CAM 192.168.0.253 CPU 0%
MEM 5%
Redundant CAM 192.168.0.254
System Name CMR_CAM2
Service Uptime 2 day(s) 0 hr(s) 13 min(s) 42 sec(s)
Active Uptime 2 day(s) 0 hr(s) 11 min(s) 31 sec(s)
System Time Fri May 20 11:38:23 IST 2011
License 1 CAS (1 used) +HA
Total 2 Users
NAC SW Version 4.9.0
HW Platform NAC 3315
Crypto HW None
Windows NAC Agent version 4.8.0.32
Mac Agent version 4.8.0.569
Web Agent version 4.8.0.4
Compliance Module version 3.4.13.1
Status Summary
Total Up Down
CAM 2 2 0
CAS 1 1 0
OOB Switch 1 1 0
Auth Server (*) 2 1 1
(*) Status of SSO based servers not considered here. Refer to Auth Servers page for their details.
Top 5 CASs
Cherry 2.2.3.10 Users 0/1500
User Summary
Users
Time(days)
role11 role4 role5 role6 Others role7
Recent Events
2011-05-20 11:38:18 Admin user session is created, login succeeded. Name:admin, Group:Full-Control Admin, IP:64.103.172.145, Login time:05/20/11 11:38:18, Last access time:05/20/11 11:38:18
2011-05-20 11:27:23 2.2.3.10 System Stats: Load factor 0 (max since reboot: 7) Mem (bytes) Total: 4116594688 Used: 538411008 Free: 3578183680 Shared: 0 Buffers: 157196288 Cached: 239857664 CPU(s) 0.0%user 0.0%nice 67.0%system 0.0%idle 0.0%iowait 0.0%irq 33.0%softirq 0.0%steal
2011-05-20 10:27:22 2.2.3.10 System Stats: Load factor 0 (max since reboot: 7) Mem (bytes) Total: 4116594688 Used: 538427392 Free: 3578167296 Shared: 0 Buffers: 157196288 Cached: 239837184 CPU(s) 0.3%user 0.0%nice 68.1%system 0.0%idle 0.0%iowait 0.0%irq 31.6%softirq 0.0%steal
2011-05-20 09:27:22 2.2.3.10 System Stats: Load factor 0 (max since reboot: 7) Mem (bytes) Total: 4116594688 Used: 538316800 Free: 3578277888 Shared: 0 Buffers: 157196288 Cached: 239820800 CPU(s) 0.3%user 0.0%nice 67.7%system 0.0%idle 0.0%iowait 0.0%irq 32.0%softirq 0.0%steal
300110

CCA Servers

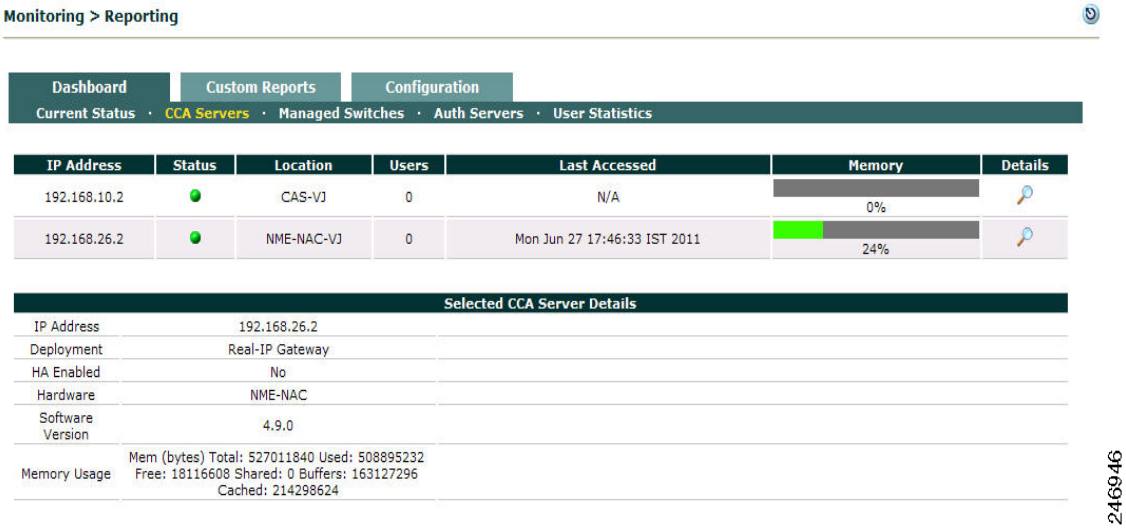
The CCA Servers view displays the details of CASs added to the CAM. It displays the online status (green if online), location, current memory usage, number of users currently connected to the CAS and last access time. Last access time is always the last successful access time for CAS by the CAM. If the CAS status is down (it would be shown in red), but the last access time would be the time CAS was last reachable.

Figure 11-15 Dashboard > CCA Servers



The details icon displays the details of selected CCA Server.

Figure 11-16 Dashboard > CCA Servers > Details



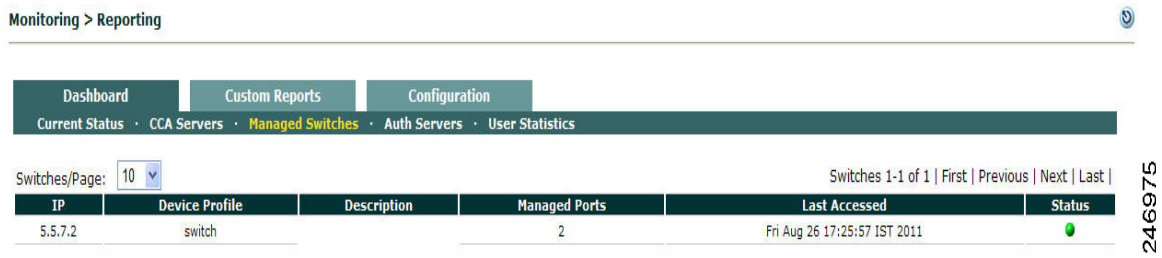
Managed Switches

The OOB switches and OOB wireless LAN controllers managed by the CAM are under Managed Switches. You can view the switch and wireless LAN controller information like its IP address, device profile, number of ports managed by CAM, status (green if online) and last access time that is last successful access time.

Note Managed ports column for wireless LAN controllers will be empty as managed ports are applicable to switches only and not to WLAN controllers.

.

Figure 11-17 Dashboard > Managed Switches

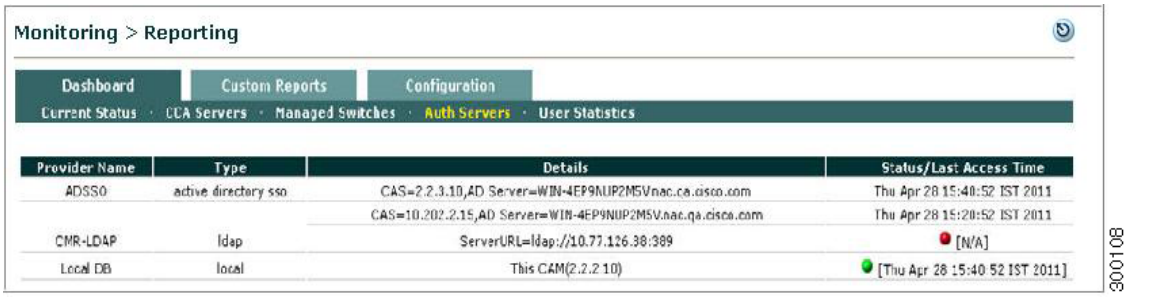


Authentication Servers

The status and other details of the authentication servers used by NAC are under the Auth Servers view. NAC does not actively check the authentication servers for their reachability to display the status here. As and when a user request comes for authentication and NAC is able to communicate to the authentication server, status is marked as reachable and the time is set as the last access time.

Two types of authentication providers are supported - First, where CAM does the active authentication with the authentication server on behalf of the end users like Radius or LDAP servers. Second, the single sign-on (SSO) type like ADSSO or VPNSSO, where the user gets authenticated elsewhere first and and an already authenticated user enters into the NAC system. In the case where the CAM does the active authentication for the end users, both the status (green if online) and the last access time is shown. In the SSO type auth providers case, CAM or NAC does not do any active authentication and hence it never tries to reach them. Accordingly, here the last access time shown is the time any user last entered into NAC using that provider. Additionally, it displays the status CAS wise that is more granular as SSO happens through CASs.

Figure 11-18 Dashboard > Auth Servers



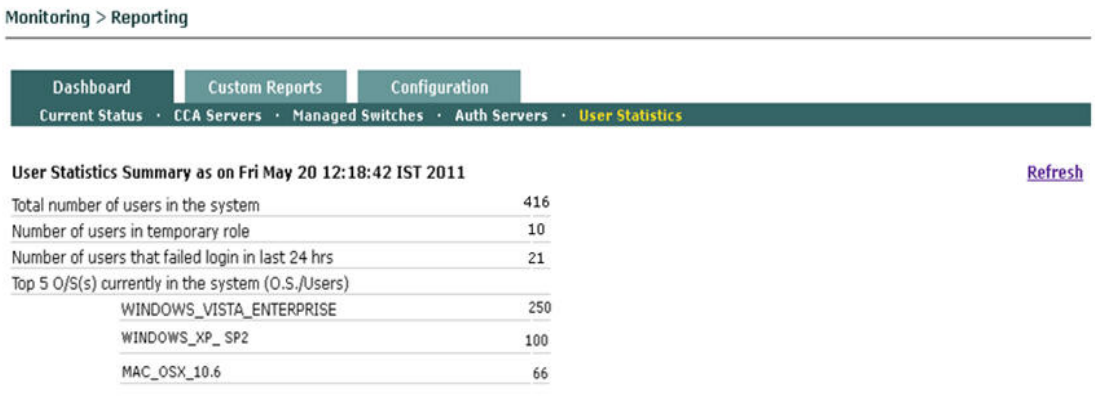
User Statistics

This tab displays the summary of current user statistics. Total number of users in the system is the total count of users currently in all roles in the systems. It includes users in temporary roles also (users undergoing posture assessment).

Number of users that failed login in the last 24 hrs is count of users who have failed login due to posture requirements only. It does not include other failures like invalid user or passwords entered by the users. Also, if the user is failing posture assessment more than once in the last 24 hrs, it is counted as one failure only.

User statistics shows the top five operating systems in current use in NAC system with respect to the number of users using those O/S(s). Click **Refresh** to get the latest data.

Figure 11-19 Dashboard > User Statistics


Monitoring > Reporting
Dashboard
Custom Reports
Configuration
Current Status · CCA Servers · Managed Switches · Auth Servers · User Statistics
User Statistics Summary as on Fri May 20 12:18:42 IST 2011
Refresh
Total number of users in the system 416
Number of users in temporary role 10
Number of users that failed login in last 24 hrs 21
Top 5 O/S(s) currently in the system (O.S./Users)
WINDOWS_VISTA_ENTERPRISE 250
WINDOWS_XP_ SP2 100
MAC_OSX_10.6 66
300111

Note When the Out-of-band devices list is large, the reporting page takes a longer time to display the reports. If this situation occurs, try deleting some of the unused devices in the Out-of-band devices list to view the reports.

Custom Reports

The **Custom Reports** tab can be used to generate customized and scheduled reports. You can save the customized settings as a template for future reference. This section contains the following topics:

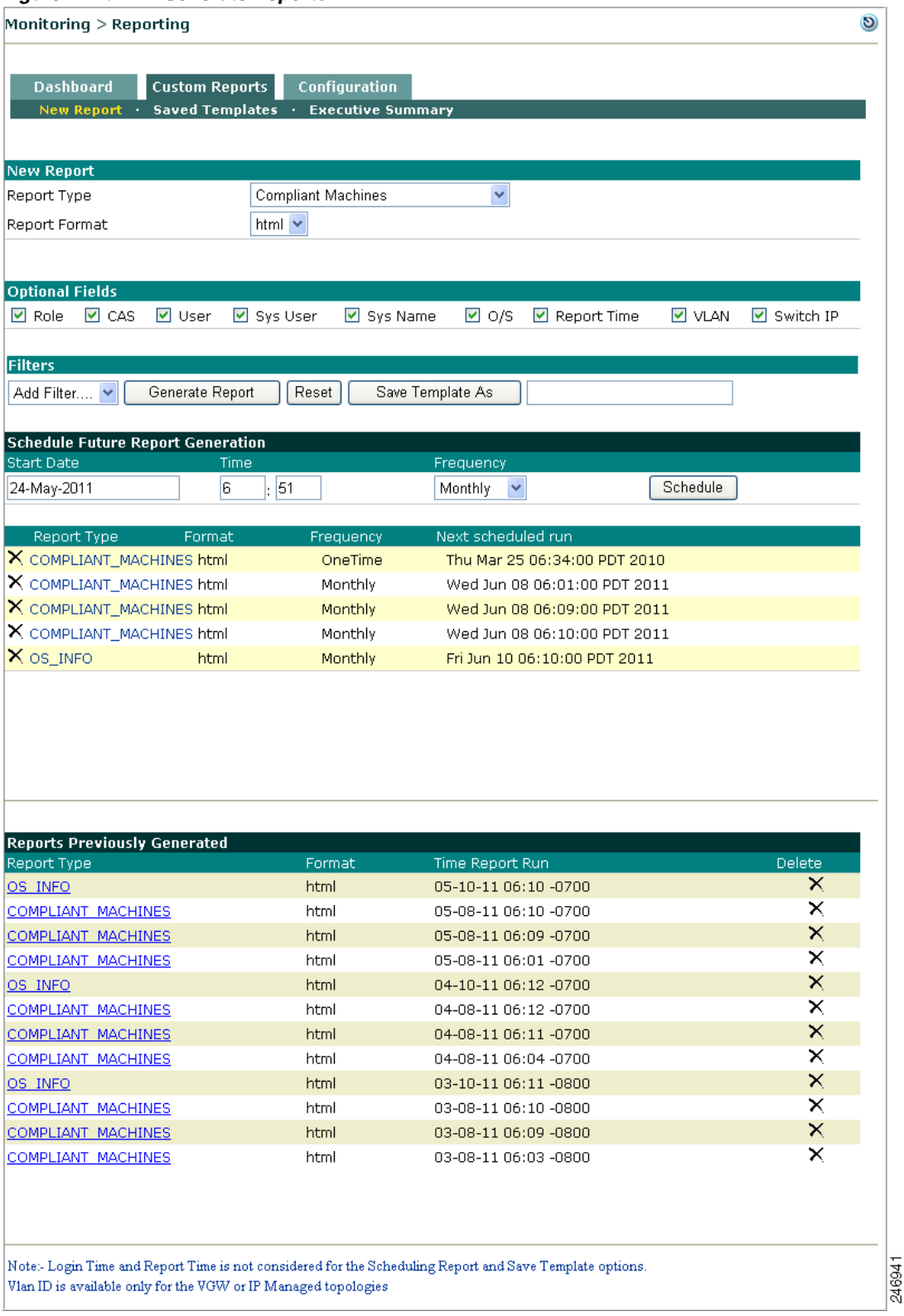
- Generate New Reports, page 11-22
- View Saved Templates, page 11-26
- View Executive Summary, page 11-26

Generate New Reports

You can generate new reports, customize them by setting up filters, and schedule to generate a report in future.

Go to **Monitoring > Reporting > Custom Reports > New Report.**

Figure 11-20 Generate Reports


Monitoring > Reporting
Dashboard
Custom Reports
Configuration
New Report · Saved Templates · Executive Summary
New Report
Report Type
Compliant Machines
Report Format
html
Optional Fields
Role CAS User Sys User Sys Name O/S Report Time VLAN Switch IP
Filters
Add Filter....
Generate Report
Reset
Save Template As
Schedule Future Report Generation
Start Date
Time
Frequency
24-May-2011
6 : 51
Monthly
Schedule
Report Type Format Frequency Next scheduled run
COMPLIANT_MACHINES html OneTime Thu Mar 25 06:34:00 PDT 2010
COMPLIANT_MACHINES html Monthly Wed Jun 08 06:01:00 PDT 2011
COMPLIANT_MACHINES html Monthly Wed Jun 08 06:09:00 PDT 2011
COMPLIANT_MACHINES html Monthly Wed Jun 08 06:10:00 PDT 2011
OS_INFO html Monthly Fri Jun 10 06:10:00 PDT 2011
Reports Previously Generated
Report Type Format Time Report Run Delete
OS_INFO html 05-10-11 06:10 -0700
COMPLIANT_MACHINES html 05-08-11 06:10 -0700
COMPLIANT_MACHINES html 05-08-11 06:09 -0700
COMPLIANT_MACHINES html 05-08-11 06:01 -0700
OS_INFO html 04-10-11 06:12 -0700
COMPLIANT_MACHINES html 04-08-11 06:12 -0700
COMPLIANT_MACHINES html 04-08-11 06:11 -0700
COMPLIANT_MACHINES html 04-08-11 06:04 -0700
OS_INFO html 03-10-11 06:11 -0800
COMPLIANT_MACHINES html 03-08-11 06:10 -0800
COMPLIANT_MACHINES html 03-08-11 06:09 -0800
COMPLIANT_MACHINES html 03-08-11 06:03 -0800
Note:- Login Time and Report Time is not considered for the Scheduling Report and Save Template options.
Vlan ID is available only for the VGW or IP Managed topologies
246941

Generating a Report

Under the **New Report** panel, you can select the **Report Type** and the required **Report Format** from the dropdown.

Report Type—Select the type of report from the drop-down list. For each type of the report, a set of fields are included in the report by default. You can include other information to the report by checking the fields that are available under **Optional Fields**.

You can select a **Filter** from the dropdown and the report is filtered by the selected option. The Filter by option varies for each Report Type.

Note When there are more than 10000 records, an empty report is generated. It is recommended to use the Filter By option to reduce the number of records to less than 10000.

Table 11-2 lists the default, optional, and filter by fields available for each report type.

Table 11-2 Report Types and the Fields Included

Report Type	Mandatory Fields[1]	Optional Fields	Filter-by Fields
Compliant Machines	IP Address, MAC Address, Login Time	Role, CAS, User, Sys User, Sys Name, O/S, Report Time, VLAN, Switch IP	All the default and optional fields
Non Compliant Machines	IP Address, MAC Address, Login Time	Role, CAS, User, Sys User, Sys Name, O/S, Report Time, VLAN, Switch IP	All the default and optional fields
Non Compliant Requirements	Requirement, MAC Address	User, Report time	All the default and optional fields
Non Compliant Users	MAC Address, User, Frequency	None	MAC address and User
A/V and A/S information	AV/AS Type, Product ID, User	Client IP, Sys Name, Software Version, Def Version, Def Date	All the default and optional fields
O/S Information	MAC Address, Sys Name, O/S, Report time	None	All the default fields
Missing A/V and A/S Requirements	User, Client IP, MAC Address, Report time	Software Version, Def Version, Def Date	Report time and all the optional fields
User Specific (Enter the User name in the text box that appears when you select this option)	Login time, Client IP, MAC Address, login success/failure flag	Role, Sys Name, Report time	All the default and optional fields
Requirement Specific (Select the Requirement from the dropdown that appears when you select this option)	Client IP, User Name, Success/Fail flag, Report time	MAC Address, Sys Name, Requirement Status	All the default and optional fields

Table 11-2 Report Types and the Fields Included (continued)

Report Type	Mandatory Fields[1]	Optional Fields	Filter-by Fields
Role Specific Reports (Select the Role from the dropdown that appears when you select this option)	Login status, User, Client IP, Requirement For each record, a link is available to view the failed and passed requirements, and the requirements in Audit / Mandatory / Optional mode.	Sys Name, Login Time, MAC Address, Requirement Status, Report time	All the default and optional fields
Controlled Switch Ports [2]	Switch IP, Port Name, User IP	Port Number, Port Description, Port Profile, User MAC Address, User Name	All the default and optional fields

1. Mandatory fields would always be part of the generated report.
2. The report is generated only when there is a maxiumum of 50 switches are available. If you have more than 50 swicthes in the network, flter the report by using the Switch IP field.

Format—Select the format of the output report file. The options available are HTML and PDF.

After selecting the Report Type, Report Format, and Filter, you can perform the following actions:

- Click **Generate Report** to generate and view the report immediately.
- Click **Reset** to remove the filters.
- Enter a name for the report and click **Save Template As** to save the current settings as a template.

Scheduling Report Generation

You can schedule to generate a report in future by setting up the date and time.

- **Start Date**—Enter the date on which the report generation has to start.
- **Time**—Enter the time at which the report generation has to start.
- **Frequency**—Select the frequency of the report generation from the drop-down list. The options available are: One Time, Hourly, Daily, Weekly, and Monthly.

Once you select the above parameters, click the **Schedule** button and the following are displayed:

- Report Type
- Format
- Frequency
- Next scheduled run

The reports are generated with the currently selected Report Type and the Report Format at the scheduled time. The previously generated reports are displayed at the bottom of the page.

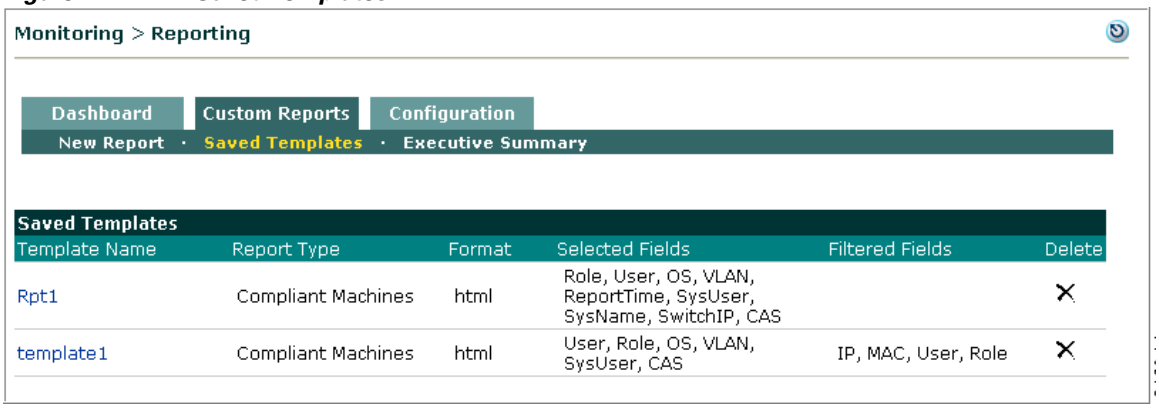
Note A maximum of 500 reports are displayed under the **Reports Previously Generated** section.

Note Login Time, Report Time, Start Date, and End Date under report Filters are not considered for Scheduled Report and Saved Template.

View Saved Templates

You can view the saved templates by navigating to **Monitoring > Reporting > Custom Reports > Saved Templates.**

Figure 11-21 Saved Templates



Clicking the **Template Name** navigates to the **New Report** tab and the saved report settings are displayed.

View Executive Summary

It displays the current license usage - number of CASs in use versus the allowed license limit, peak user count in the last 24 hrs versus the allowed license limit. It also displays the role-wise compliance statistics summary - how many users failed login and how many passed login. Go to **Monitoring > Reporting > Custom Reports > Executive Summary** to view a report of the NAC License Utilization and Role-wise compliance statistics as shown in Figure 11-22.

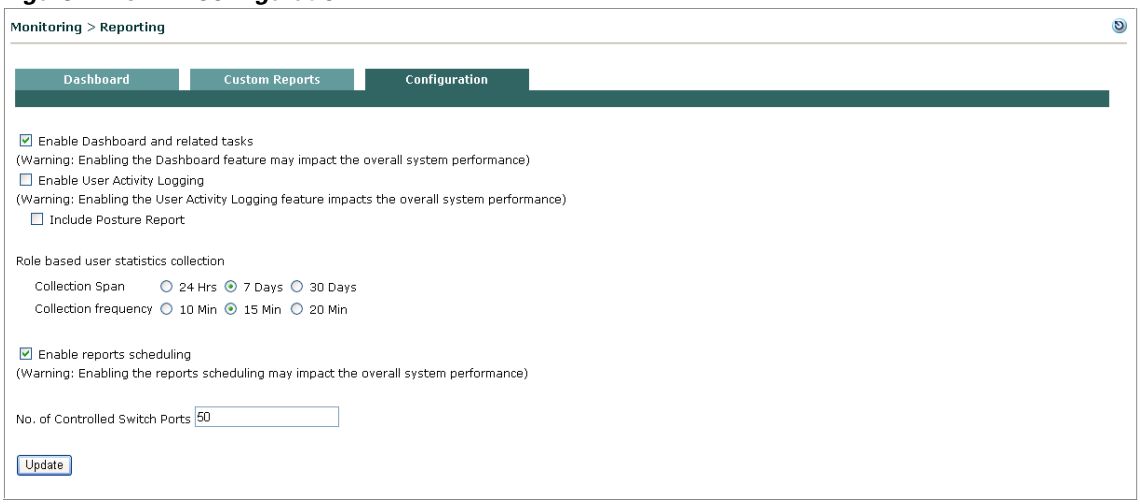
Figure 11-22 Executive Summary



Configuration

Use the **Monitoring > Reporting > Configuration** tab to enable Dashboard and Custom Reports.

Figure 11-23 Configuration


Monitoring > Reporting
Dashboard
Custom Reports
Configuration
Enable Dashboard and related tasks
(Warning: Enabling the Dashboard feature may impact the overall system performance)
Enable User Activity Logging
(Warning: Enabling the User Activity Logging feature impacts the overall system performance)
Include Posture Report
Role based user statistics collection
Collection Span 24 Hrs 7 Days 30 Days
Collection frequency 10 Min 15 Min 20 Min
Enable reports scheduling
(Warning: Enabling the reports scheduling may impact the overall system performance)
No. of Controlled Switch Ports 50
Update
360488

- Check the **Enable Dashboard and related tasks** checkbox to enable the Dashboard page.
- Check the **Enable User Activity Logging** checkbox to save the user information in the User Activity Log (UAL) files.
  - Enabling **Include Posture Report** in UAL logging seriously impacts system performance.
- Role based user statistics collection: NAC periodically collects role-wise user count statistics. Choose the **Collection Span** and **Collection frequency** for role-wise statistics collection. Statistics collected by NAC is used to generate the user summary chart in the main dashboard (current status page).
  - Choose the period of time for the **Collection Span**. The User Statistics is displayed for the selected period. Choose the **Collection frequency** and the User Statistics is refreshed at the interval of the selected frequency.
- Check **Enable reports scheduling** to enable scheduling of reports in the **Custom Reports** tab.
- Enter the **No. of Controlled Switch Ports**. This switch count is used to generate the final report of Contolled Switch ports.

Click **Update** to save the settings.

User Activity Log Files

User Activity Log (UAL) Files are the log files that record user activities. This is an XML file stored in the location: **/perfigo/control/data/ual/**.

The user information is stored in this file only when the **Enable User Activity Logging** checkbox is enabled in the **Monitoring > Reporting > Configuration** tab. The data is logged according to the period of interval set in the Current Status tab.

The UAL files are updated with the user information every day and the historical data for the past 90 days are available in the file.

The following details are stored in the UAL files:

- Username
- Activity Time—login time, logout time, or role change time
- Activity Reason—Reason for logout. The reasons may be “Logout”, “Timeout”, or “Admin Action”
- User Location—VPN, switch, port, VLAN, etc. (whatever is applicable)
- User Reports—Applicable for login and role change, not on logout
- Activity Result— The result is reported as success or failure. If activity fails, it means the login has failed. Activity Reason is supplied with the appropriate agent, authentication server, or switch management error
- MAC address
- Hostname
- IP address
- Role
- OS
- VLAN
- Session Length—For role change and logout only (applicable for only In-Band deployments). Session Length is a pre-configured value for the temporary role configured under **User Management > User Roles> Schedule**.

Note Session Length will not be displayed in the Logout activity when the client is logged out from a Temporary Role after failing to satisfy a requirement.

Note The UAL file is not updated when the **Enable User Activity Logging** checkbox is unchecked in the **Monitoring > Reporting > Configuration** tab.

Online Users list

Two **Online Users** lists are viewed from the **Monitoring > Online Users > View Online Users** tab:

- **In-Band Online Users**
  - Tracks In-Band authenticated users logged into the network. In-Band users with active sessions on the network are listed by characteristics such as IP address, MAC address (if available), authentication provider, and user role.
  - Removing a user from the In-Band Online Users list logs the user off of the In-Band network.
- **Out-of-Band Online Users**
  - Tracks all authenticated Out-of-Band users that are on the Access VLAN (trusted network). Out-of-Band users can be listed by switch IP address, port, and assigned Access VLAN, in addition to client IP address, MAC address (if available), authentication provider, and user role.

- Removing a user from the Out-of-Band Online Users list causes the VLAN of the port to be changed from the Access VLAN to the Authentication VLAN. You can additionally configure the Port profile to bounce the port (for a Real-IP gateway). See Out-of-Band Users, page 11-31 and Out-of-Band Users, page 3-68 for details.

Both **Online Users** lists are based on the IP address of users. Note that:

- For Layer 2 deployments the **User MAC** address field is valid
- For Layer 3 deployments the **User MAC** address field is **not** valid (for example, 00:00:00:00:00:00)

Only the Certified Devices List is based on client MAC addresses, and therefore the Certified Devices List never applies to users in Layer 3 deployments.

For Out-of-Band deployments, OOB user entries always appear first in the In-Band Online Users list, then in the Out-of-Band Online Users list. When user traffic is coming from a controlled port of a managed switch, the user shows up first in the In-Band Online Users list during the authentication process, then is moved to the Out-of-Band Online Users list after the user is authenticated and moved to the Access VLAN.

Finally, the **Display Settings** tab let you choose which user characteristics are displayed on each respective **Online Users** page.

Note When a user device is connecting to Cisco NAC Appliance from behind a VPN3000/ASA device, the MAC address of the first physical adapter that is available to the CAS/CAM is used to identify the user on the Online Users list. This may not necessarily be the adapter with which the user is connecting to the network. Users should **disable** the wireless interface of their machines when connecting to the network using the wired (Ethernet card) interface.

Interpreting Active Users

Once logged onto the Cisco NAC Appliance network, an active user session persists until one of the following events occurs:

- The user logs out of the network through the browser logout page or Agent logout.

  Once on the network, users can remain logged on after a computer shutdown/restart. A user can log out of the network using the web logout page or Agent logout.

- The Agent user logs off Windows or shuts down Windows machine.

  You can configure the CAM and Agent to log off In-Band users only from the Clean Access system when the user logs off from the Windows domain (i.e. **Start > Shutdown > Log off current user**) or shuts down the machine (**Start > Shutdown > Shutdown machine**).

- An administrator manually drops the user from the network.

  The **Monitoring > Online Users > View Online Users** page (IB or OOB) can be used to drop users from the network, without deleting their clients from the Certified Devices List.

- The session times out using the Session Timer.

  The Session Timer works the same way for multi-hop L3 (IB) deployments as for L2 (IB or OOB) deployments and is set in **User Management > User Roles> Schedule > Session Timer**. It is set per user role, and logs out any user in the selected role from the network after the configured time has elapsed. For details, see Configure Session Timer (per User Role), page 8-17.

- The CAS determines that the user is no longer connected using the Heartbeat Timer and the CAM terminates the session.

The Heartbeat Timer applies to L2 IB deployments only and is set for all users regardless of role. It can be set globally for all Clean Access Servers using the form **User Management > User Roles> Schedule > Heartbeat Timer**, or for a specific Clean Access Server using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer**. For details, see Configure Heartbeat Timer (User Inactivity Timeout), page 8-17.

The Heartbeat Timer will not function in L3 deployments, and does not apply to OOB users. However, note that the HeartBeat Timer will work if the CAS is the first hop behind the VPN concentrator. This is because the VPN concentrator responds to the ARP queries for the IP addresses of its current tunnel clients.

- The Certified Device list is cleared (automatically or manually) and the user is removed from the network.

  The Certified Devices List applies to L2 (IB or OOB) deployments only and can be scheduled to be cleared automatically and periodically using the global Certified Devices timer form (**Device Management > Clean Access > Certified Devices > Timer**). You can manually clear the certified devices for a specific Clean Access Server from the Certified Devices List using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Filters > Clean Access > Certified Devices,** or manually clear the Certified Device list across all Clean Access Servers using the global form **Device Management > Clean Access > Certified Devices**. For details, see Manage Certified Devices, page 11-10.

  Keep in mind that the Certified Devices List will not display remote VPN/L3 clients (since these sessions are IP-based rather than MAC address-based).

- SSO and Auto-Logout are configured for the VPN concentrator, and the user disconnects from the VPN.

  With Auto Logout enabled, when the user disconnects from the VPN client, the user is automatically removed from the Online Users list (In-Band).

  Note that when SSO is configured for multi-hop L3 VPN concentrator integration, if the user's session on the CAS times out but the user is still logged in on the VPN concentrator, the user will be able to log back into the CAS without providing a username/password.

Note Whether the CAS or another server is used for DHCP, if a user's DHCP lease expires, the user remains on the Online Users list (In-Band or Out-of-Band). When the lease expires, the client machine will try to renew the lease.

See also Configure User Session and Heartbeat Timeouts, page 8-15 and Out-of-Band Users, page 3-68 for additional details.

View Online Users

The **View Online Users** tab provides two links for the two online users lists: **In-Band** and **Out-of-Band**.

By default, **View Online User** pages display the login user name, IP and MAC address (if available), provider, and role of each user. For information on selecting the column information to display, such as OS version, or for Out-of-Band users: switch port, see Display Settings, page 11-35.

A *green* background for an entry indicates a user device accessing the Clean Access network in a temporary role: either a Quarantine role or the Agent Temporary role.

A *blue* background for an entry indicates a user device accessing the Clean Access network in a restricted network access role.

A device listed on the **View Online Users** page but not in the Clean Access **Certified Devices List** generally indicates the device is in the process of certification.

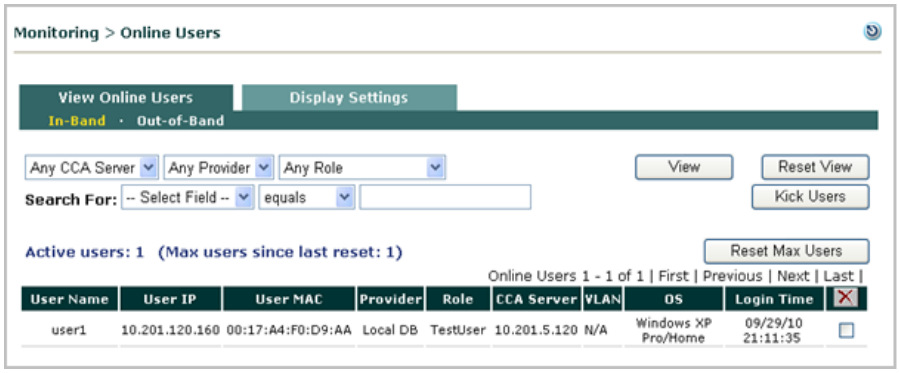
In-Band Users

Clicking the **In-Band** link brings up the **View Online Users** page for In-Band users (Figure 11-24). The In-Band Online Users list tracks the In-Band users logged into the Clean Access network.

The Clean Access Manager adds a client IP and MAC address (if available) to this list after a user logs into the network either through web login or the Agent.

Removing a user from the Online Users list logs the user off the In-Band network.

Figure 11-24 View Online Users Page—In-Band



Note For AD SSO users, the **Provider** field displays `AD_SSO`, and the **User/User Name** field lists both the username and domain of the user (for example, `user1@domain.name.com`.) on the **Online Users** and **Certified Devices** pages.

Out-of-Band Users

Clicking the **Out-of-Band** link brings up the **View Online Users** page for Out-of-Band users (Figure 11-25).

The Out-of-Band Online Users list tracks all Out-of-Band authenticated users that are on the Access VLAN (on the trusted network). The CAM adds a user IP address to the Out-of-Band Online Users list after a client is switched to the Access VLAN.

Note **The "User IP" of Out-of-Band online users will be the IP address of the user on the Authentication VLAN. By definition CCA does not track users once they are on the Access VLAN; therefore OOB users are tracked by the Auth VLAN IP address they have while in the CCA network.**

When a user is removed from the Out-of-Band Online Users list, the following typically occurs:

1. The CAM bounces the switch port (off and on).
2. The switch resends SNMP traps to the CAM.
3. The CAM changes the VLAN of the port based on the configured Port Profile associated with this controlled port.

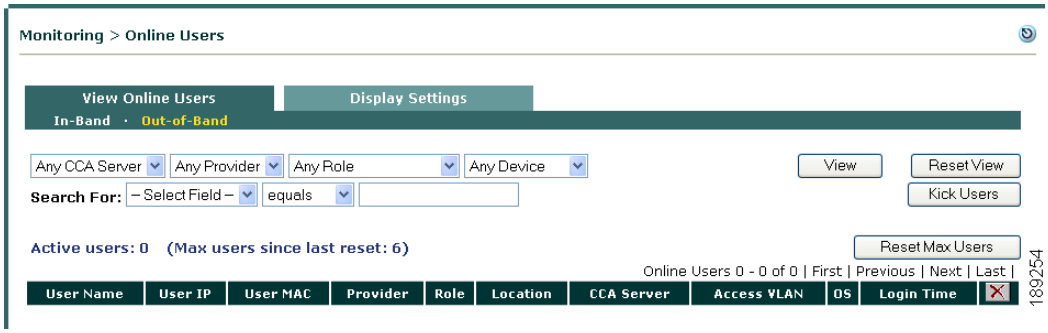
Note Removing an OOB user from the Certified Devices List also removes the user from Out-of-Band Online Users list and changes the port from the Access VLAN to the Auth VLAN.

Note When the "**Remove Out-of-Band online user without bouncing port**" option is checked for the Port Profile, for OOB Virtual Gateways, the switch port will not be bounced when:

- Users are removed from the Out-of-Band Online Users list, or
- Devices are removed from the Certified Devices list

Instead, the port Access VLAN will be changed to the Authentication VLAN (see Add Port Profile, page 3-34 for details).

Figure 11-25 View Online Users Page—Out-of-Band



Note For AD SSO users, the **Provider** field displays `AD_SSO`, and the **User/User Name** field lists both the username and domain of the user (for example, `user1@domain.name.com`.) on the **Online Users** and **Certified Devices** pages.

For more details, see Chapter 3, "Switch Management: Configuring Out-of-Band Deployment."

Table 11-3 describes the search criteria, information/navigation elements, and options for removing user.s from the online users pages. Note that clicking a column heading sorts entries on the page by the column.

Table 11-3 View Online Users Page Controls

Item	Description
User Name	The user name used for login is displayed.

Table 11-3 View Online Users Page Controls

Item		Description
Search Criteria:	**CCA Server**	• Any Clean Access Server • <specific CAS IP address>
	Provider	• Any Provider • <specific authentication provider>
	Role	• Any Role • Unauthenticated Role • Temporary Role • Quarantine Role • <specific Role>
	Location	• Any Switch or Wireless LAN Controller • <specific switch/WLC IP address>
	Select Field	• User Name • IP Address • MAC Address
	Operator	**equals**: Search text value must be an exact match for this operator **starts with:** **ends with:** **contains**:
	Search Text	Enter the value to be searched using the operator selected.
Controls:	**View**	After selecting the search criteria, click **View** to display the results. You can view users by CAS, provider, user role, user name, IP address, MAC address (if available), or switch (OOB only).
	Reset View	Resets to the default view (with search criteria reset to "Any")
	Kick Users	**Clicking Kick Users** terminates all user sessions filtered through the search criteria across the number of applicable pages. Users can be selectively dropped from the network by any of the search criteria used to **View** users. The "filtered users indicator" shown in Figure 11-25 displays the total number of filtered users that will be terminated when **Kick Users** is clicked.
	Reset Max Users	Resets the maximum number of users to the actual number of users displayed in the "Active users:" status field (Figure 11-25)
	Delete Checked Entries	You can remove as many users as are shown on the **page** by selecting the checkbox next to each user and clicking the **Delete Checked Entries** Icon.
Navigation:	**First/Previous/Next/Last**	These navigation links allow you to page through the list of online users. A maximum of 25 entries is displayed per page.

View Users by Clean Access Server, Authentication Provider, or Role

1. From the **View Online Users** page, select a specific Clean Access Server, or leave the first field as **Any CCA Server**.
2. Select a specific authentication provider, or leave as **Any Provider**.
3. Select a specific user role, or leave as **Any Role**.
4. Click **View** to display users by Clean Access Server, provider, role or any combination of the three.

Search by User Name, IP, or MAC Address

1. In the **Select Field** dropdown menu next to **Search For:**, select **User Name** or **IP Address** or **MAC Address**.
2. Select one of the four operators: **starts with**, **ends with**, **contains**, **exact match**.
3. Enter the text to be searched in the **Search For:** text field. If using the **exact match** operator, only the exact match for the search text entered is returned.
4. Click **View** to display results.

Log Users Off the Network

Clicking **Kick Users** terminates all user sessions filtered through the search criteria across the number of applicable pages. (Note that a maximum of 25 entries is displayed per page.) You can selectively remove users from the network by any of the search criteria used to **View** users. The "filtered users indicator" shown in Figure 11-24 displays the total number of filtered user sessions that will be terminated when you click the **Kick Users** button.

1. Go to **Monitoring > Online Users > View Online Users**.
2. To terminate user sessions either:
   - Drop all users (filtered through search criteria) from the network by clicking **Kick Users**
   - Drop individual users by selecting the checkbox next to each user and clicking the **Delete Checked Entries** Icon.

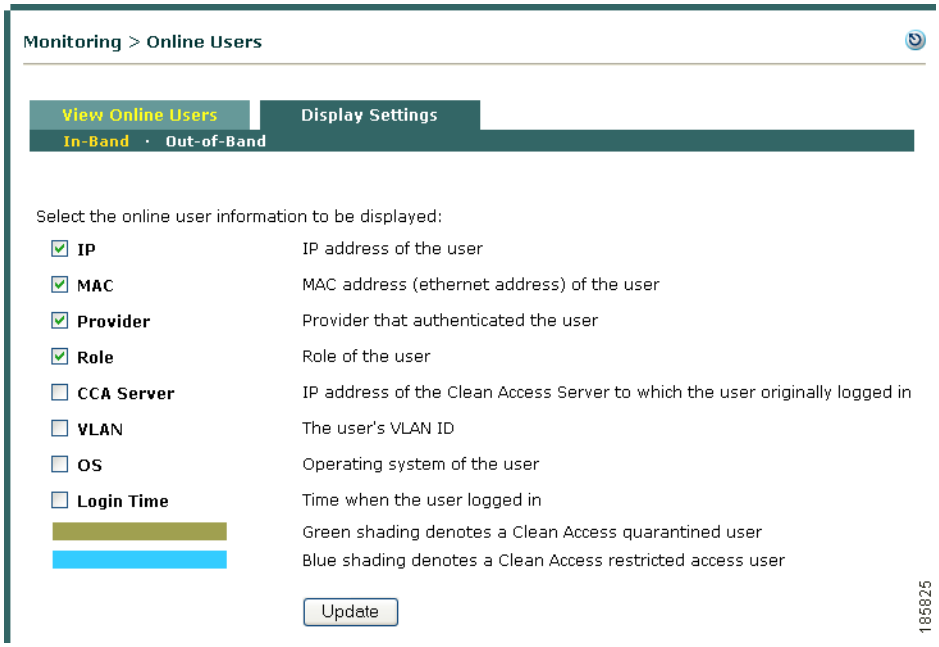
Note that removing a user from the online users list (and the network) does not remove the user from the **Certified Devices List**. However, dropping a user from the Certified Devices List also logs the user off the network. See Clear Certified or Exempt Devices Manually, page 11-13 for further details.

Note When there is a large number Out-of-Band Online Users, then the **Kick User** option takes a longer time to remove the online users. This happens when switches and CASs are not available to the CAM, resulting in a timeout for each communication failure. The **Kick User** is slow due to this timeout.

Display Settings

Figure 11-26 shows the **Display Settings** page for In-Band users.

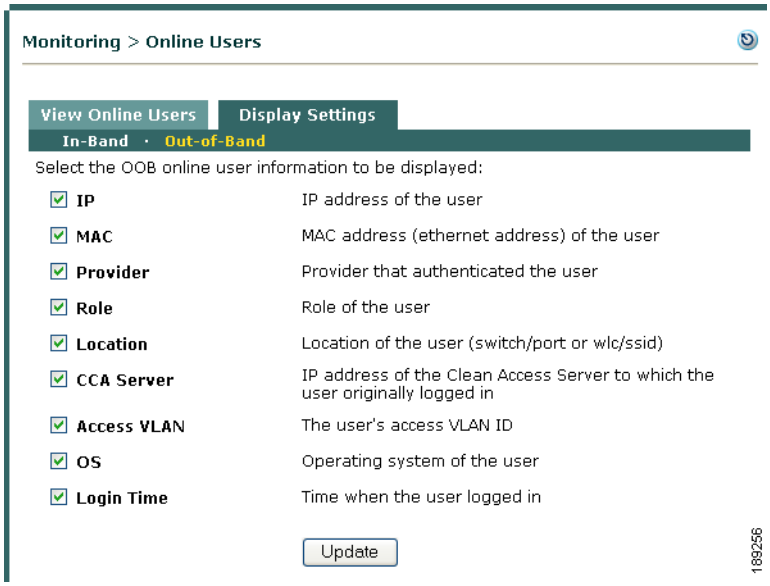
Figure 11-26 Display Settings—In-Band


Monitoring > Online Users
View Online Users
Display Settings
In-Band · Out-of-Band
Select the online user information to be displayed:
IP
IP address of the user
MAC
MAC address (ethernet address) of the user
Provider
Provider that authenticated the user
Role
Role of the user
CCA Server
IP address of the Clean Access Server to which the user originally logged in
VLAN
The user's VLAN ID
OS
Operating system of the user
Login Time
Time when the user logged in
Green shading denotes a Clean Access quarantined user
Blue shading denotes a Clean Access restricted access user
Update
185825

Note **Role**—the role assigned to the user upon login.

Figure 11-27 shows the **Display Settings** page for Out-of-Band users.

Figure 11-27 Display Settings—Out-of-Band



To choose what information is displayed on the View Online Users page:

Step 1 Click the **Display Settings** tab.

Step 2 Select the check box next to an item to display it in the list.

Step 3 Click **Update**.

Step 4 Click the **View Online Users** tab to see the desired settings displayed.

Agent Troubleshooting

This section contains the following:

- Debug Logging for Cisco NAC Appliance Agents
- Client Cannot Connect/Login
- No Agent Pop-Up/Login Disabled
- Client Cannot Connect (Traffic Policy Related)
- AV/AS Rule Troubleshooting
- Cisco NAC Web Agent Status Codes
- Known Issue for Windows Script 5.6
- Known Issue for MS Update Scanning Tool (KB873333)

Debug Logging for Cisco NAC Appliance Agents

This section describes how to view and/or enable debug logging for Cisco NAC Appliance Agents. Refer to the following sections for steps for each Agent type:

- Generate Cisco NAC Agent Debug Logs
- Cisco NAC Web Agent Logs
- Generate Mac OS X Agent Debug Log

Copy these event logs to include them in a customer support case.

Generate Cisco NAC Agent Debug Logs

To generate Cisco NAC Agent logs using the Cisco Log Packager utility, refer to Create Agent Log Files Using the Cisco Log Packager, page 11-6.

Cisco NAC Web Agent Logs

The Cisco NAC Web Agent version 4.1.3.9 and later can generate logs when downloaded and executed. By default, the Cisco NAC Web Agent writes the log file upon startup with debugging turned on. The Cisco NAC Web Agent generates the following log files for troubleshooting purposes: **webagent.log** and **webagentsetup.log**. These files should be included in any Cisco Technical Assistance Center (TAC) support case for the Web Agent. Typically, these files are located in the user's temp directory, in the form:

C:\Document and Settings\<*user*>\Local Settings\Temp\webagent.log

C:\Document and Settings\<*user*>\Local Settings\Temp\webagentsetup.log

If these files are not visible, check the TEMP environment variable setting. From a command-prompt, type “echo %TEMP%” or “cd %TEMP%”.

When the client uses Microsoft Internet Explorer, the Cisco NAC Web Agent is downloaded to the **C:\Documents and Settings\<*user*>\Local Settings\Temporary internet files** directory.

Generate Mac OS X Agent Debug Log

For Mac OS X Agents, the Agent **event.log** file and **preference.plist** user preferences file are available under <*username*> **> Library > Application Support > Cisco Systems > CCAAgent.app**. To change or specify the LogLevel setting, however, you must access the global **setting.plist** file (which is *different* from the user-level **preference.plist** file).

Because Cisco does not recommend allowing individual users to change the LogLevel value on the client machine, you must be a superuser or root user to alter the global **setting.plist** system preferences file and specify a different Agent LogLevel.

Note For versions prior to 4.1.3.0, debug logging for the Mac OS X Agent is enabled under <*local drive ID*> **> Library > Application Support > Cisco Systems | CCAAgent.app > Show Package Contents > setting.plist**.

To view and/or change the Agent LogLevel:

Step 1 Open the navigator pane and navigate to <*local drive ID*> **> Applications**.

Step 2 Highlight and right-click the **CCAAgent.app** icon to bring up the selection menu.

Step 3 Choose **Show Package Contents > Resources**.

Step 4 Choose **setting.plist**.

Step 5 If you want to change the current LogLevel setting using Mac **Property Editor** (for Mac OS 10.5 and later), find the current LogLevel Key and replace the exiting value with one of the following:

- **Info**—Include only informational messages in the event log
- **Warn**—Include informational and warning messages in the event log
- **Error**—Include informational, warning, and error messages in the event log
- **Debug**—Include all Agent messages (including informational, warning, and error) in the event log

Note The **Info** and **Warn** entry types only feature a few messages pertaining to very specific Agent events. Therefore, you will probably only need either the **Error** or **Debug** Agent event log level when troubleshooting Agent connection issues.

Note Because Apple, Inc. introduced a binary-format .plist implementation in Mac OS 10.4, the .plist file may not be editable by using a common text editor such as vi. If the .plist file is not editable (displayed as binary characters), you either need to use the Mac **Property List Editor** utility from the Mac OS X CD-ROM or acquire another similar tool to edit the **setting.plist** file.

Property List Editor is an application included in the Apple Developer Tools for editing .plist files. You can find it at <*CD-ROM*>/Developer/Applications/Utilities/Property List Editor.app.

If the **setting.plist** file *is* editable, you can use a standard text editor like vi to edit the LogLevel value in the file.

You must be the root user to edit the file.

Client Cannot Connect/Login

The following client errors at login can indicate CAM/CAS certificate related issues (i.e. the CAS does not trust the certificate of the CAM, or vice-versa):

- Users attempting web login continue to see the login page after entering user credentials and are not redirected.
- Users attempting Agent login see the following error: “Clean Access Server could not establish a secure connection to the Clean Access Manager at <*IPaddress or domain*>.

To resolve these issues, refer to Troubleshooting Certificate Issues, page 14-21.

No Agent Pop-Up/Login Disabled

For L2 or L3 deployments, the Agent will pop up on the client if “Popup Login Window” is enabled on the Agent and the Agent detects it is behind the Clean Access Server. If the Agent does not pop up, this indicates it cannot reach the CAS.

To Troubleshoot L2 Deployments:

1. Make sure the client machine can get a correct IP address. Open a command tool (Start > Run > cmd) and type `ipfconfig` or `ipconfig /all` to check the client IP address information.
2. If necessary, type `ipconfig /release`, then `ipconfig /renew` to reset the DHCP lease for the client.

To Troubleshoot L3 Deployments:

1. Check whether the Discovery Host field is set to the IP address of the CAM itself under **Device Management > Clean Access > Clean Access Agent > Installation | Discovery Host**. This field must be the address of a device on the trusted side and cannot be the address of the CAS.
2. Uninstall the Agent from the client machine.
3. Change the **Discovery Host** field to the IP address of the CAM and click **Update**.
4. Reboot the CAS.
5. Re-download and re-install the Agent on the client.

Note The **Login** option on the Agent is correctly disabled (greyed out) in the following cases:

- For OOB deployments, the Agent user is already logged in through the CAS and the client port is on the Access VLAN.
- For multi-hop L3 deployments, Single Sign-On (SSO) has been enabled and the user has already authenticated through the VPN concentrator (therefore is already automatically logged into Cisco NAC Appliance).
- MAC address-based authentication is configured for the machine of this user and therefore no user login is required.

Client Cannot Connect (Traffic Policy Related)

The following errors can indicate DNS, proxy or network traffic policy related issues:

- User can login via Agent, but cannot access web page/Internet after login.
- User cannot access web login page without typing in https://<CAS_IP_address> as the URL.

To troubleshoot these issues:

- Verify and/or change **DNS Servers** setting on the CAS (under **Device Management > CCA Servers > Manage <CAS_IP> > Network > DNS**)
- If enabling the CAS as a DHCP server, verify and/or change the **DNS Servers** field for the Subnet List (under **Device Management > CCA Servers > Manage <CAS_IP> > Network > DHCP > Subnet List > List | Edit**).
- If remediation sites cannot be reached after login, verify default host policies (Allowed Hosts) are enabled for the Temporary role (under **User Management > User Roles > Traffic Control > Host**).
- If using a proxy server, make sure a traffic policy allowing HTTP traffic to the proxy server is enabled for the Temporary role. Verify the proxy is correctly set in the browser (from IE go to Tools > Internet Options > Connections > LAN Settings | Proxy server).

See Troubleshooting Host-Based Policies, page 8-29 for additional details.

AV/AS Rule Troubleshooting

To view administrator reports for the Agent, go to **Device Management > Clean Access > Clean Access Agent > Reports**. To view information from the client, right-click the Agent taskbar icon and select **Properties**.

When troubleshooting AV/AS Rules, please provide the following information:

1. Version of CAS, CAM, and Agent.
2. Client OS version (e.g. Windows XP SP2)
3. Name and version of AV/AS vendor product.
4. What is failing—AV/AS installation check or AV/AS update checks? What is the error message?
5. What is the current value of the AV/AS def date/version on the failing client machine?
6. What is the corresponding value of the AV/AS def date/version being checked for on the CAM? (See **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.)

Cisco NAC Web Agent Status Codes

Table 11-4 shows the status codes passed from the ActiveX or Java Applet downloader used to install the Cisco NAC Web Agent on the client machine.

Table 11-4 Java Server Page Status Codes from ActiveX Control or Java Downloader Applet

ActiveX/Java Applet Status Code	Value/Description
ACTIVEX_FAILURE	-1 “unable to launch active-x control”
DL_FAILURE	-2 “failed to download the web agent executable”
EXE_FAILURE	-3 “there was an error running the web agent”
ACTIVEX_START	0
STATUS_DL_START	1
DL_IN_PROGRESS	2
EXE_IN_PROGRES	3

Table 11-5 shows the status codes passed from the Cisco NAC Web Agent back to the Cisco NAC Appliance system during posture assessment and remediation.

Table 11-5 Cisco NAC Web Agent Status Codes

Cisco NAC Web Agent Status Code	Value
COMPLIANT/SUCCESS	32
NON_COMPLIANT	33
REJECTED_AUP	34
REMEDIATION TIMEOUT	35
GENERAL ERROR	36
TEMPORARY/RESTRICTED ACCESS	37
WEB AGENT ALREADY RUNNING	38

Known Issue for Windows Script 5.6

Windows Script 5.6 is required for proper functioning of the Agent. Most older operating systems come with Windows Script 5.1 components. Microsoft automatically installs the new 5.6 component on performing Windows updates. Windows installer components 2.0 and 3.0 also require Windows Script 5.6. However, PC machines with a fresh install of Windows 2000 that have never performed Windows updates will not have the Windows Script 5.6 component. Cisco NAC Appliance cannot redistribute this component as it is not provided by Microsoft as a merge module/redistributable.

In this case, administrators will have to access the MSDN website to get this component and upgrade to Windows Script 5.6. For convenience, links to the component from MSDN are listed below:

Filename: **scripten.exe**

URL:
http://www.microsoft.com/downloads/en/details.aspx?FamilyId=01592C48-207D-4BE1-8A76-1C4099D7BBB9&displaylang=en

If these links change on MSDN, try a search for the file names provided above or search for the phrase "Windows Script 5.6."

Known Issue for MS Update Scanning Tool (KB873333)

Background

KB873333 is a critical update that is required for Windows XP Professional and Home for SP1 and SP2. It fixes an OS vulnerability that can allow remote code to run. However, Microsoft had a bug in this hotfix which caused problems on SP2 editions (home/pro). This bug required another fix (KB894391), because KB873333 on SP2 caused a problem with displaying Double Byte Character Sets (DBCS). However, KB894391 does not replace KB873333, it only fixes the DBCS display issue.

Ideally, KB894391 should not be installed or shown in updates unless the user machine has KB873333. However, the MS Update Scanning Tool tool shows it irrespective of whether or not KB873333 is installed. In addition, if due to ordering of the updates, KB894391 is installed, the MS Update Scanning Tool does not show KB873333 as being installed, thereby leaving the vulnerability open. This could happen if the user does not install KB873333 and only selects KB894391 to install from the updates list shown or manually installs KB894391 without installing KB873333 first. In this case, the next time updates are run, the user will not be shown KB873333 as a required update, because the MS Update Scanning Tool (including MS Baseline Analyzer) will assume KB873333 is installed if KB894391 is installed, even if this is not true and the machine is still vulnerable.

Workaround

Because of this potential vulnerability, Cisco does not intend to remove the update check for KB87333 from the Clean Access ruleset and users should manually download and install KB873333 to protect their machines. This can be done in one of two ways:

Option 1 (Cisco Recommended Option)

Create a new Link requirement in the CAM web console to check for KB873333, using the following steps:

1. Create a rule to check for the presence of KB873333. To create this rule, go to the Rules section of the web console and click New Rule. Give the rule a name (e.g. “KB873333_Rule”), and for the rule expression, copy/paste the exact name of the KB873333 check from the list of checks displayed on that page (the list of available checks appear below the new rule creation section). Save the rule by clicking “Add Rule.”
2. Download the update executable for KB873333 from Microsoft's website and host it on an available web server.
3. Create a Link Requirement on Cisco NAC Appliance, and enter the URL from step 2.
4. Create Requirement-Rules for this requirement by selecting the rule you created in step 1.
5. Finally, go to the Role-Requirements section, and associate the Requirement you just created with the role to which you want this to be applied.



Note On the Requirements page, make sure that the KB873333 requirement is above the Windows Hotfixes requirement.

Option 2

Uninstall KB894391 from affected machines. After rebooting, go to the Windows Update page again. Windows Update should now display both the updates. Install KB873333 and KB894391 on the client machine. Note that this requires administrators to educate users or manually perform this task on the user machines.



Configuring Network Scanning

Note **Nessus-based network scanning capabilities only apply to users accessing the Cisco NAC Appliance network via UNIX operating system-based client machines. The Cisco NAC Agent does not support Nessus-based network scanning.**

This chapter describes how to set up network scanning for Cisco NAC Appliance. Topics include:

- Overview, page 12-1
- User Page Summary, page 12-4
- Configure the Quarantine Role, page 12-6
- Load Nessus Plugins into the Clean Access Manager Repository, page 12-6
- Configure General Setup, page 12-9
- Apply Plugins, page 12-10
- Configure Plugin Options, page 12-12
- Configure Vulnerability Handling, page 12-13
- Test Scanning, page 12-16
- Customize the User Agreement Page, page 12-19
- View Scan Reports, page 12-17

Overview

The Cisco NAC Appliance network scanner uses Nessus plugins to check for security vulnerabilities. With Cisco NAC Appliance, you can define automatic, immediate responses to scan results. For example, if a vulnerability is found, you can have the user notified, blocked from the network, or assigned to a quarantine role.

Nessus (http://www.nessus.org), an open source project for security-related software, provides plugins designed to test for specific vulnerabilities on a network. In addition to plugins for remotely detecting the presence of particular worms, plugins exist for detecting peer-to-peer software activity or web servers. The following description defines Nessus plugins:

> *Nessus plugins are very much like virus signatures in a common virus scanner application. Each plugin is written to test for a specific vulnerability. These can be written to actually exploit the vulnerability or just test for known vulnerable software versions. Plugins can be written in most any*

language but usually are written in the Nessus Attack Scripting Language (NASL). NASL is Nessus' own language, specifically designed for vulnerability test writing. Each plugin is written to test for a specific known vulnerability and/or industry best practices. NASL plugins typically test by sending very specific code to the target and comparing the results against stored vulnerable values.

— Anderson, Harry. "Introduction to Nessus" October 28, 2003
http://www.securityfocus.com/infocus/1741 (10/29/04).

Note Cisco NAC Appliance supports the launching of Nessus plugins only and does not support the Nessus plugins themselves.

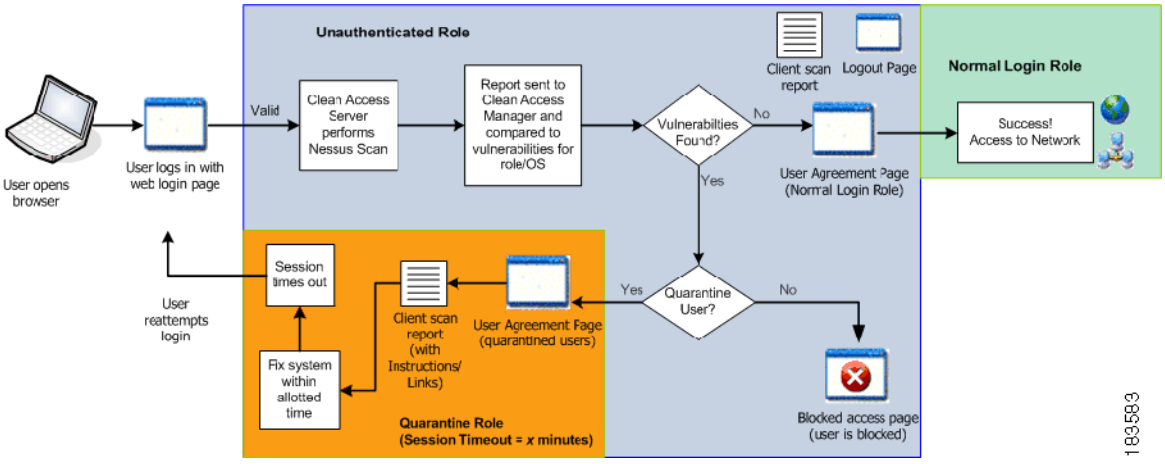
You can use most standard Nessus plugins with Cisco NAC Appliance. You can also customize plugins or create your own using NASL. Refer to the Nessus website for information on how to create plugins using NASL.

When scanning is performed, the network scanner scans the client system according to the plugins you selected and generates a standard report to the Clean Access Manager containing the results of the scan. Network scanning reports will indicate whether the plugin resulted in a security hole, warning, or system information (according to how the Nessus plugin was written). The Clean Access Manager then interprets the report by comparing the result of the plugin to the vulnerability definition you have configured for it. If the report result matches the result you have configured as a vulnerability, the event is logged under **Monitoring > Event Logs > View Logs**, and you can also configure the following options:

- Show the result of the scan to the user.
- Block the user from the network
- Put the user in the quarantine role for limited access until the client system is fixed.
- Warn the user of the vulnerability (with the User Agreement Page).

Figure 12-1 illustrates the general network scanning client assessment process when a user authenticates via web login. If both the Agent and network scanning are enabled for a user role, the user follows the sequence shown in Figure 10-1 on page 10-2 then in Figure 12-1 for the network scanning portion. In this case, the Agent dialogs provide the user information where applicable.

Figure 12-1 Network Scanning Client Assessment



Network Scanning Implementation Steps

The following sections describe the steps required to set up network scanning:

Step 1 Configure the Quarantine Role, page 12-6

Step 2 Load Nessus Plugins into the Clean Access Manager Repository, page 12-6

Step 3 Configure General Setup, page 12-9

Step 4 Apply Plugins, page 12-10

Step 5 Configure Plugin Options, page 12-12

Step 6 Configure Vulnerability Handling, page 12-13

Step 7 Test Scanning, page 12-16

Step 8 Customize the User Agreement Page, page 12-19

Step 9 View Scan Reports, page 12-17

User Page Summary

Table 12-1 summarizes the web pages that appear to users during the course of login and perform Nessus Scanning, and lists where they are configured in the web admin console.

Table 12-1 User Page Summary

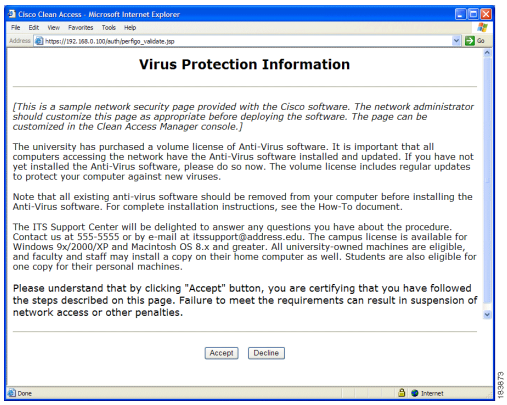
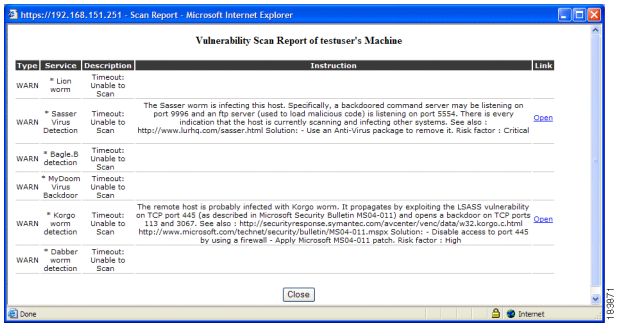
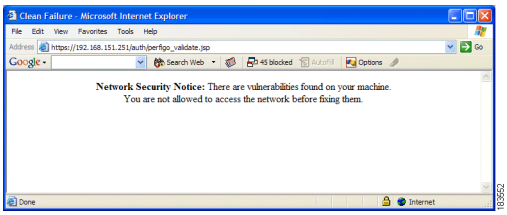
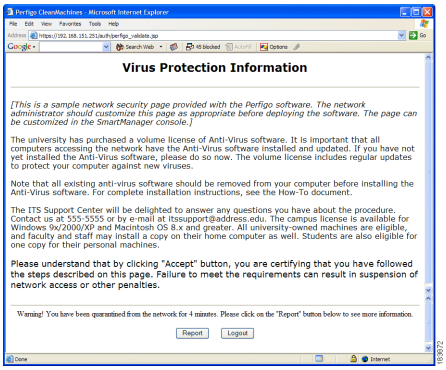
Page	Configured in:	Purpose
Web Login /Network Scanner User Pages		
Network Scanning User Agreement Page	Enable in: **Device Management > Clean Access > General Setup > Web Login** Configure page in: **Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement** See Customize the User Agreement Page, page 12-19	If enabled, this page appears after a web login user authenticates and passes network scanning. The user must click **Accept** to access the network. 
Scan Vulnerability Report	Enable in: **Device Management > Clean Access > General Setup > Web Login** Configure page in: **Device Management > Clean Access > Network Scanner > Scan Setup > Vulnerabilities** See Configure Vulnerability Handling, page 12-13	If enabled, this client report appears to web login users after network scanning results in vulnerabilities. It can also be accessed as a link from the Logout page. Administrators can view the admin version of the client report from **Device Management > Clean Access > Network Scanner > Reports**. Agent users with network scanning vulnerabilities see this information in the context of Agent dialogs. The report appears as follows: 

Table 12-1 User Page Summary (continued)

Page	Configured in:	Purpose
Block Access Page	**Device Management > Clean Access > General Setup > Web Login** See Customize the User Agreement Page, page 12-19.	If enabled, a web login user sees this page if blocked from the network when vulnerabilities are found on the client system after network scanning, 
User Agreement Page: quarantined user, original role	Enable in: **Device Management > Clean Access > General Setup > Web Login** Configure page in: **Network Scanner > Scan Setup > User Agreement** Select **normal login** role. See Customize the User Agreement Page, page 12-19.	If enabled, this page appears to a web login user if quarantined when vulnerabilities are found on the client system after network scanning.  This page has the same **Information Page Message (or URL)** contents ("Virus Protection Information") as the User Agreement Page for the normal login role. However, the **Acknowledgment Instructions** are hardcoded to include the Session Timeout for the original role, and button labels are hardcoded as "**Report**" and "**Logout**".
User Agreement Page: **quarantined user, quarantine role**	Enable in: **Device Management > Clean Access > General Setup > Web Login** Configure page in: **Network Scanner > Scan Setup > User Agreement** Select appropriate **quarantine** role. See Customize the User Agreement Page, page 12-19.	If enabled, this page appears to a web login user if quarantined when vulnerabilities are found on the client system after network scanning. This page allows you to specify a User Agreement Page just for the quarantine role, (as opposed to using the quarantine version of the User Agreement Page for the normal login role, as described above). The **Acknowledgment Instructions** are hardcoded to include the Session Timeout for the quarantine role, and the button labels are also hardcoded as "**Report**" and "**Logout**".

For additional information on redirecting users by role to specific pages or URLs (outside of Cisco NAC Appliance), see Create Local User Accounts, page 6-15.

For additional Cisco NAC Appliance configuration information, see Configure General Setup, page 12-9.

For additional details on configuring Agent Requirements, see Configuring Agent-Based Posture Assessment, page 9-39.

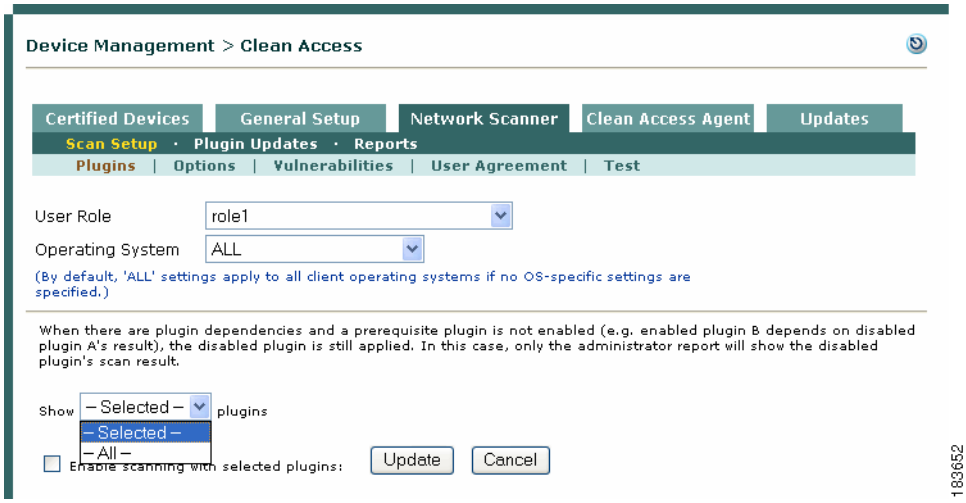
Configure the Quarantine Role

See Configure Network Scanning Quarantine Role, page 8-21 for details.

Load Nessus Plugins into the Clean Access Manager Repository

When the Clean Access Manager is first installed, its Nessus scan plugin repository is empty (Figure 12-2). Plugins in the repository are listed under **Device Management > Clean Access > Network Scanner > Scan Setup > Plugins**. You can manually load plugins you have downloaded from the Nessus website—as a combined **plugins.tar.gz** file or as individual .nasl files—to the Clean Access Manager's plugin repository. You can also load .nasl plugins that you have created yourself.

Figure 12-2 Network Scanner Plugins Page


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
User Role
role1
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.
Show
– Selected –
plugins
– Selected –
– All –
Enable scanning with selected plugins:
Update
Cancel
183652

Note Due to a licensing requirement by Tenable, Cisco is not able to bundle pre-tested Nessus plugins or automated plugin updates to Cisco NAC Appliance, effective Release 3.3.6/3.4.1. Customers can still download Nessus plugins selectively and manually through http://www.nessus.org.
For details on Nessus plugin feeds, see http://www.nessus.org/plugins/index.php?view=feed.
To facilitate the debugging of manually uploaded plugins, see Show Log, page 12-17.

Note Most Nessus 2.2 plugins are supported and can be uploaded to the Clean Access Manager. You must register for Nessus 2.2 plugins from http://www.nessus.org/plugins/index.php?view=register. Once you register, you will be able to download the free plugins. Nessus version 2.2.7 has a NASL_LEVEL value of less than 3004. Cisco NAC appliance does not support Nessus plugins which require the NASL_LEVEL to be equal to or greater than 3004. Cisco NAC Appliance currently does not support Nessus version 3.0 and later plugins.

If a plugin you want to add has dependent plugins, you must load those dependencies or the plugin is not applied. When customizing a plugin, Cisco recommends giving the plugin a unique name, so that it is not overwritten later by a plugin in a Nessus update set.

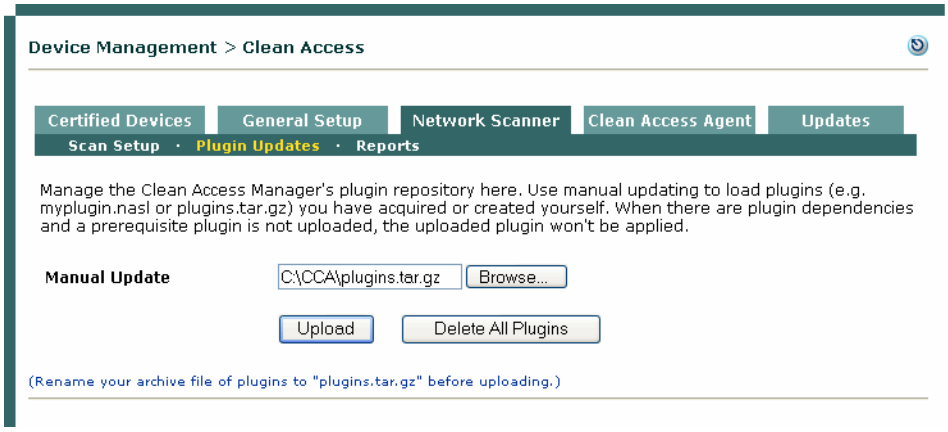
The plugin's description appears in the **Plugins** form of the **Scan Setup** submenu (Figure 12-4 on page 12-8). By customizing the plugin's description, you enable admin console users to distinguish the plugin from others in the plugin set.

Plugins that you have loaded are automatically published from the Clean Access Manager repository to the Clean Access Servers, which perform the actual scanning. The CAM distributes the plugin set to the Clean Access Servers as they start up, if the CAS version of the plugin set differs from the CAM version.

Uploading Plugins

1. Go to **Device Management > Clean Access > Network Scanner > Plugin Updates**.

Figure 12-3 Plugin Updates

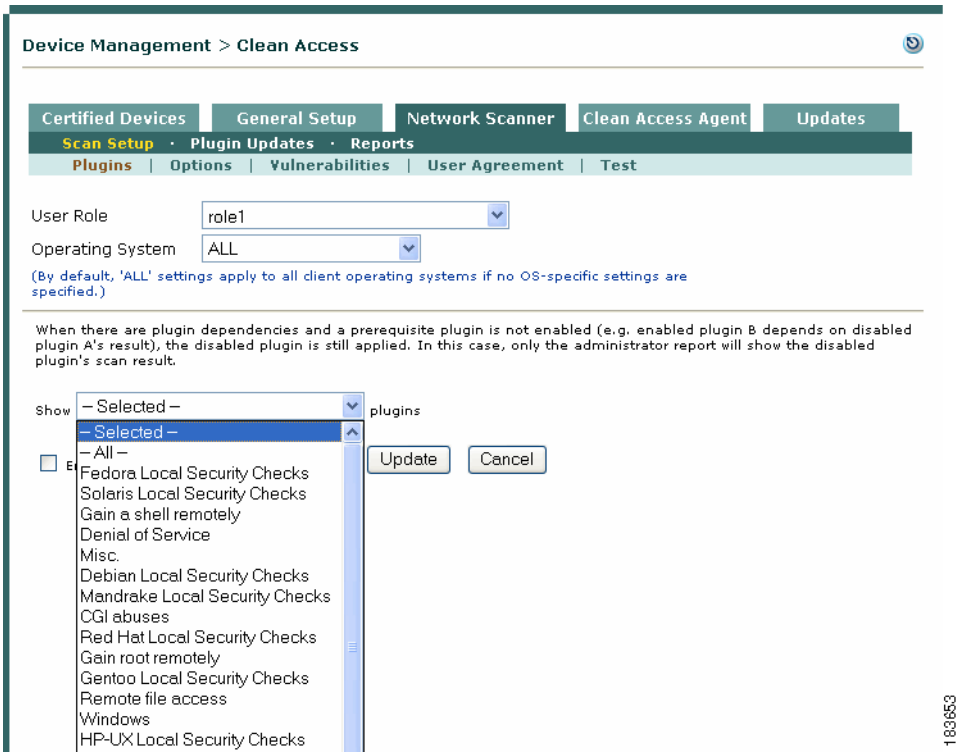

Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Scan Setup · Plugin Updates · Reports
Manage the Clean Access Manager's plugin repository here. Use manual updating to load plugins (e.g. myplugin.nasl or plugins.tar.gz) you have acquired or created yourself. When there are plugin dependencies and a prerequisite plugin is not uploaded, the uploaded plugin won't be applied.
Manual Update
C:\CCA\plugins.tar.gz
Browse...
Upload
Delete All Plugins
(Rename your archive file of plugins to "plugins.tar.gz" before uploading.)
183649

2. With the plugin file in a location accessible to the computer on which you are working, click the **Browse** button next to the **Manual Update** field and navigate to the plugin archive file (**plugins.tar.gz**) or individual plugin file (**myplugin.nasl**).

Note The filename of the uploaded nessus plugin archive must be **plugins.tar.gz**. Most Nessus 2.2 plugins are supported. Nessus version 2.2.7 has a NASL_LEVEL value of less than 3004. Cisco NAC appliance does not support Nessus plugins which require the NASL_LEVEL to be equal to or greater than 3004. Cisco NAC Appliance currently does not support Nessus version 3 plugins due to vendor licensing restrictions.

3. Click **Upload**.
4. The list of plugins loaded to the repository displays under **Network Scanner > Scan Setup > Plugins** (Figure 12-4).

Figure 12-4 Plugins Page After Upload


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
User Role
role1
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.
Show
– Selected –
plugins
– Selected –
– All –
Fedora Local Security Checks
Solaris Local Security Checks
Gain a shell remotely
Denial of Service
Misc.
Debian Local Security Checks
Mandrake Local Security Checks
CGI abuses
Red Hat Local Security Checks
Gain root remotely
Gentoo Local Security Checks
Remote file access
Windows
HP-UX Local Security Checks
Update
Cancel
183653

Note The default view on the **Plugins** page is "**Selected**." If Nessus plugins have not yet been checked and updated for the user role, the default view (i.e. Selected Plugins) shows no plugins. To view the plugins you have uploaded, choose one of the other views (for example, "All," "Backdoors," etc.) from the "Show...Plugins" dropdown.

5. If the plugins do not immediately display after **Upload**, click **Delete All Plugins**, then perform the upload again.
6. Apply the plugin and configure its parameters as described in the following sections:
   - Apply Plugins, page 12-10
   - Configure Vulnerability Handling, page 12-13.

Note When there are plugin dependencies and a prerequisite plugin is not uploaded, the uploaded plugin will not be applied.

Deleting Plugins

1. Go to **Device Management > Clean Access > Network Scanner > Plugin Updates**.
2. Click the **Delete All Plugins** button to remove all plugins from the repository. The **Network Scanner > Scan Setup > Plugins** page will no longer be populated.

Configure General Setup

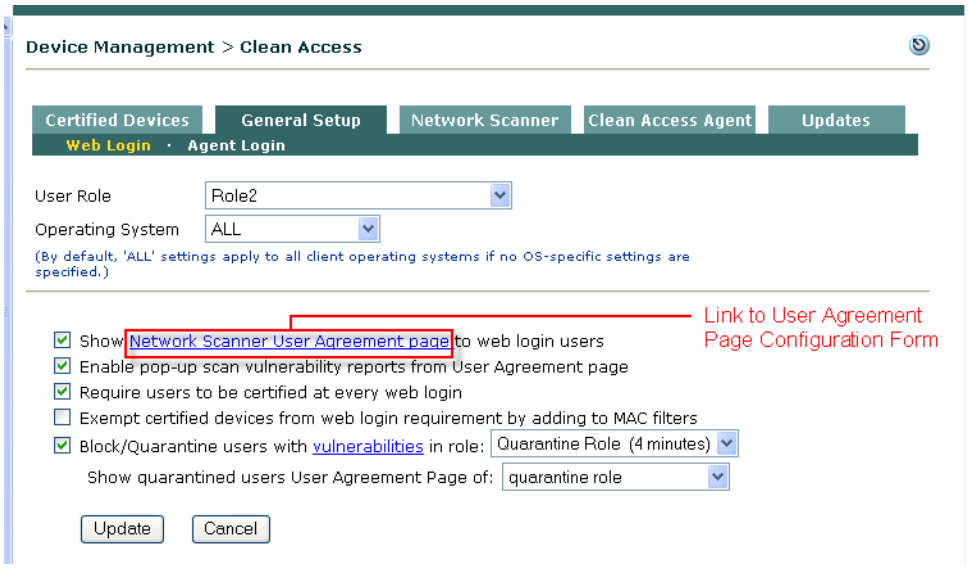
After loading the scan plugins, you can configure scanning by user role and operating system. Before starting, make sure user roles appropriate for your environment are created.

The General Setup page provides general controls to configure user roles and operating systems for network scanning, including whether user agreement or scan report pages pop up, and whether a client is blocked or quarantined if found with vulnerabilities.

To configure network scanning user page options:

1. Go to **Device Management > Clean Access > General Setup> Web Login**.

Figure 12-5 General Setup—Web Login


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Web Login · Agent Login
User Role
Role2
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
Link to User Agreement Page Configuration Form
Show Network Scanner User Agreement page to web login users
Enable pop-up scan vulnerability reports from User Agreement page
Require users to be certified at every web login
Exempt certified devices from web login requirement by adding to MAC filters
Block/Quarantine users with vulnerabilities in role:
Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of:
quarantine role
Update
Cancel
183648

2. Choose the role for which you want to configure scanning from the **User Role** dropdown.
3. Similarly, choose the user operating system to which the configuration applies from the **Operating System** dropdown. You can apply settings to all versions of an OS platform (such as WINDOWS_ALL), or to a specific operating system version (such as WINDOWS_XP). ALL settings will apply to a client system if a configuration for the specific version of that user's operating system does not exist.

   If providing specialized settings, select the operating system and clear the checkbox for the ALL setting (for example, deselect "**Use 'ALL' settings for the WINDOWS OS family if no version-specific settings are specified"**).
4. Enable the network scanning options:
   - **Show Network Scanner User Agreement page to web login users**
   - **Enable pop-up scan vulnerability reports from User Agreement page**
   - **Require users to be certified at every web login**—this forces clients to go through network scanning at each login (otherwise, clients go through scanning only the first time they log in.)

- **Exempt certified devices from web login requirement by adding to MAC filters**—(Optional) this allows users that have met network scanning requirements to bypass web login altogether by adding the MAC address of their machines to the device filters list.
- **Block/Quarantine users with vulnerabilities in role**—either:

  Select the quarantine role in which to quarantine the user, or

  Select block access to block the user from the network and modify the contents (if desired) of the blocked access page that will appear.

5. When finished, click **Update** to save your changes to the user role.

For additional details, see Client Login Overview, page 1-6 and Customize the User Agreement Page, page 12-19.

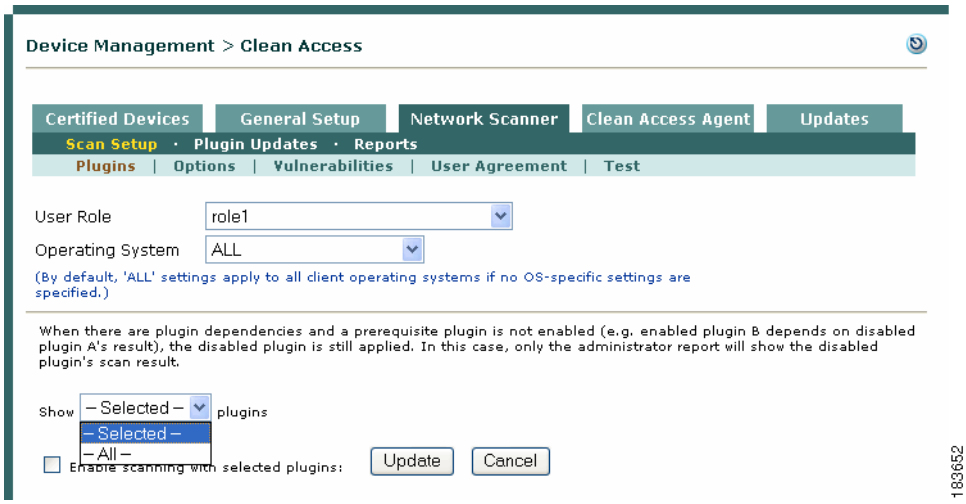
Apply Plugins

Select the Nessus plugins to be used to determine client vulnerabilities from the **Plugins** page. Select the user role and operating system and choose the plugins that participate in scanning.

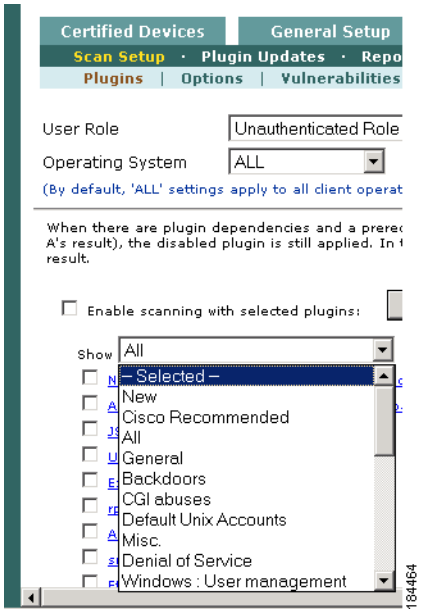
To apply scanning plugins:

1. Go **Network Scanner > Scan Setup > Plugins**.

Figure 12-6 Plugins


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
User Role
role1
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
When there are plugin dependencies and a prerequisite plugin is not enabled (e.g. enabled plugin B depends on disabled plugin A's result), the disabled plugin is still applied. In this case, only the administrator report will show the disabled plugin's scan result.
Show
– Selected –
plugins
– Selected –
– All –
Enable scanning with selected plugins:
Update
Cancel
183652

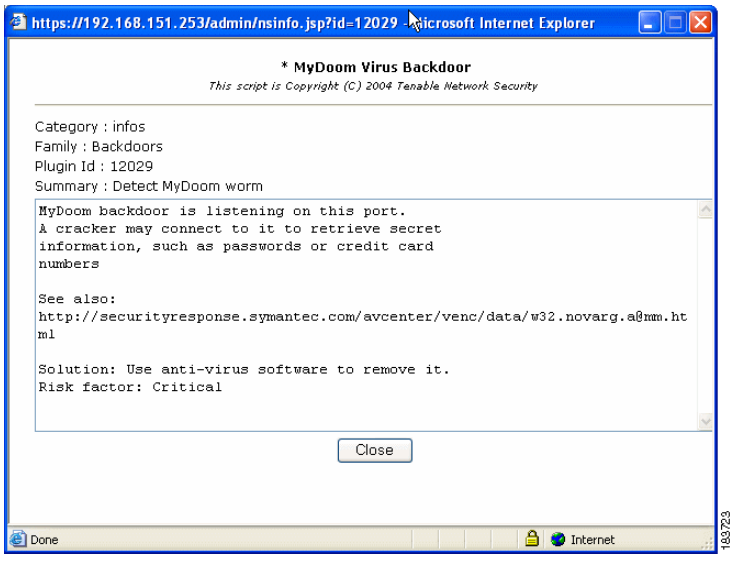
2. In the form, select a **User Role** and **Operating System**, and check the **Enable scanning with selected plugins** check box.
3. If you have many plugins in the repository, you can filter which are displayed at a time by choosing a plugin family from the plugins list, as shown below.
   - Selecting **All** displays all plugins in the repository.
   - Choosing **- Selected-** displays only the plugins you already chose and enabled for the role.



Note The default view on the Nessus plugin page (**Device Management > Clean Access > Network Scanner > Scan Setup > Plugins**) is "**Selected**." Note that if Nessus plugins have not yet been checked and updated for the user role, the default view (i.e. Selected Plugins) shows no plugins. To select plugins, the administrator must choose one of the other views (for example, "All," "Backdoors," etc.) from the "Show...Plugins" dropdown.

4. Click the plugin name for details. An information dialog appears for each plugin (Figure 12-7).

Figure 12-7 Nessus Plugin Description



5. Select the check box for each plugin that you want to participate in the scan for that role.

Note If the plugin is dependent on other plugins in the repository, those plugins are enabled automatically.

6. When finished, click **Update**. This transfers the selected plugins to the **Vulnerabilities** page so that you can configure how these vulnerabilities are handled if discovered on a client system.

If the plugin has configurable parameters, you can now use the **Options** form to configure them, as described in the following procedures. Otherwise you can continue to Configure Vulnerability Handling, page 12-13.

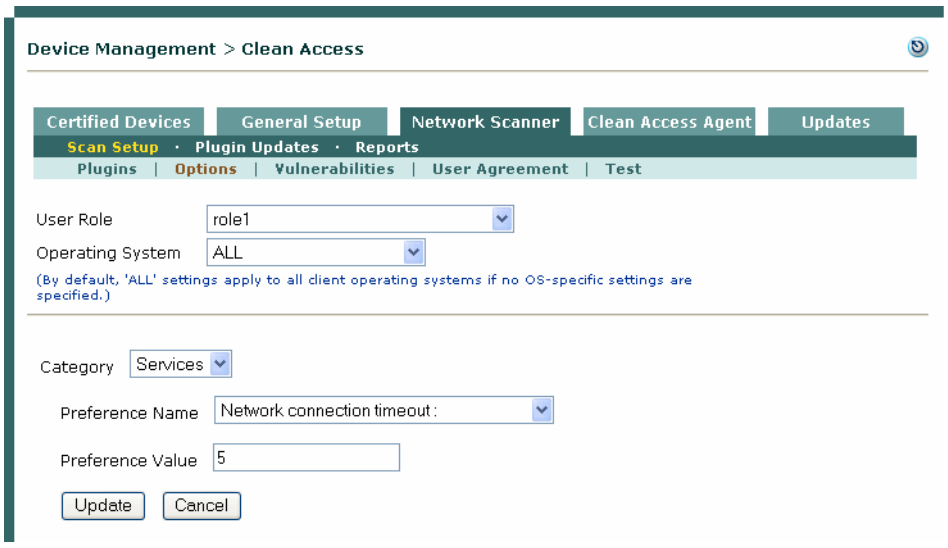
Configure Plugin Options

For plugins that support input parameters, you can configure parameters in the **Options** form. Before starting, the plugin must be enabled in the **Plugins** form, as described in Apply Plugins, page 12-10.

To configure plugin options:

1. In the **Network Scanner** tab, click the **Scan Setup** submenu link, then open the **Options** form.
2. With the appropriate role and operating system selected, choose the plugin you want to configure from the **Plugin** list. All plugins enabled for the role appear in the list.
3. Choose the option you want to configure for the plugin from the options list. When you select a configurable option, **Category**, **Preference Name**, and **Preference Value** dropdowns and/or text boxes will display, as applicable for the option. Parameters that cannot be configured are indicated by a "Not supported" message.

Figure 12-8 Options



4. From the dropdown menus, select the **Category** and **Preference Name**, type the **Preference Value** (if applicable), and click **Update**. Note that you need to click **Update** for each parameter you configure.

Note Cisco recommends using the Agent for host registry checks. In order to use Nessus Windows registry checks, you will need to have a common account (with access to the registry) on all the machines you want to check. This can be configured under **Device Management > Clean Access > Network Scanner > Scan Setup > Options |** Category: **Login configurations |** Preference Name: **[SMB account/domain/password]**. For details on Nessus 2.2 Windows registry checks (requiring credentials), refer to http://www.nessus.org/documentation/nessus_credential_checks.pdf.

Configure Vulnerability Handling

If scanning uncovers a vulnerability on the user's system, the user can be blocked from the network, quarantined, or only warned about the vulnerability.

Network scan reports are listed by user logon attempt under **Device Management > Clean Access > Network Scanner > Reports**. Client scan reports can be enabled by selecting the **Enable pop-up scan vulnerability reports from User Agreement page** option from **Device Management > Clean Access > General Setup.**

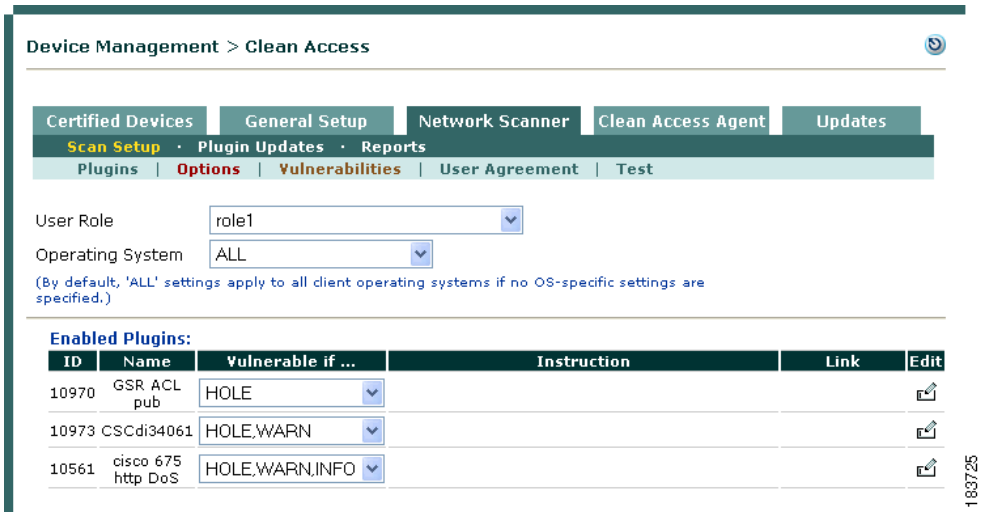
If enabled, a client scan report will appear in a popup window to notify users if a vulnerability result was found. This client report is a subset of the scan report and lists only vulnerability results along with instruction steps or a URL link that guide the user through remediation for the vulnerability. If browser popups are blocked on the user's system, the user can click the **Scan Report** link on the logout page to view the report. The warning text that appears to users for each vulnerability is configurable, as described in the following procedures.

Note that typically, plugins do not return results when no issue is found. If a client goes through network scanning and no vulnerability results are found, no scan report popup is displayed.

To configure how vulnerabilities are handled:

1. Open the **Network Scanner > Scan Setup > Vulnerabilities** form.
2. Select a **User Role** and **Operating System**. Note that plugins selected apply to the User Role:OS pair. The same set of plugins appears for all operating systems in the role. However, you can customize which plugins are considered vulnerabilities per operating system.

Figure 12-9 Vulnerabilities



3. For Enabled Plugins (plugins that have been enabled through the Plugins menu) select the following:

   ID: This is the number of the plugin that will be listed on the scan report.

   Name: Name of the plugin.

   Vulnerable if: These dropdown controls configure how the Clean Access Manager interprets the scan result for the plugin. If the client is scanned and the result returned for a plugin matches the vulnerability configuration, the client will be put in the quarantine role (or blocked). You can increase or decrease the level of result that triggers a vulnerability and assigns users to the quarantine role.

   1. **NEVER**—Ignore the report for the plugin. Even if a HOLE, WARN, or INFO result appears on the report, this plugin is never treated as vulnerability and will never cause the user to be put in the quarantine role.
   2. **HOLE**—If HOLE is the result for this plugin, the client has this vulnerability and will be put in the quarantine role. A result of WARN or INFO on the report is not considered a vulnerability for this plugin. In most cases, administrators should select "HOLE" to configure vulnerabilities. "HOLE" will ignore the other types of information (if any) reported by plugins.
   3. **HOLE, WARN** (Timeout)—This setting means the following:

      A HOLE result for this plugin is considered a vulnerability and the client will be put in the quarantine role.

      A WARN result for this plugin is considered a vulnerability and the client will be put in the quarantine role. A WARN result means the plugin scan timed out (due to personal firewalls or other software) and could not be performed on the machine. Choosing WARN as a vulnerability will quarantine any client that has a firewall enabled. However, it can also be used as a precautionary measure to quarantine clients when the results of the scan are not known.

      An INFO result on the report is not considered a vulnerability for this plugin.
   4. **HOLE, WARN, INFO**—This setting means the following:

      A HOLE result for this plugin means the client has this vulnerability and will be put in the quarantine role.

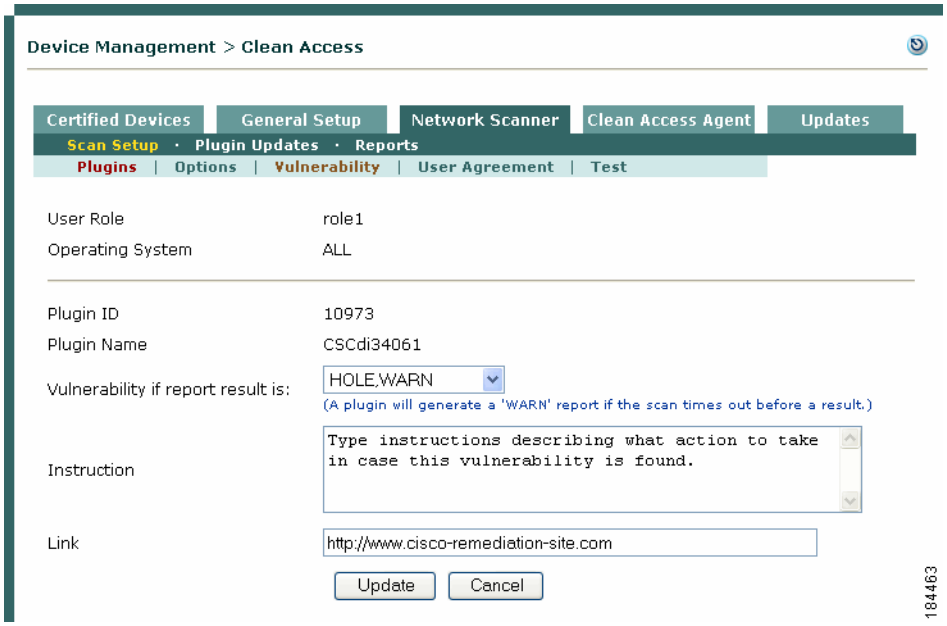
      A WARN result for this plugin is considered a vulnerability and the client will be put in the quarantine role. An WARN result usually indicates a client that has a firewall enabled.

An INFO result on the report is considered a vulnerability and the client will be put in the quarantine role. An INFO result indicates status information such as what services (e.g. Windows) may running on a port, or NetBIOS information for the machine. Choosing this level of vulnerability will quarantine any client that returns status information.

Note If the plugin does not return INFO results (and there are no HOLE or WARN results), the client will not be quarantined.

5. To edit a plugin, click the **Edit** icon next to the plugin that you want to configure.
6. The **Edit Vulnerabilities** form appears.

Figure 12-10 Edit Vulnerability



7. From the **Vulnerability if report result is:** option menu, you can increase or decrease the level of vulnerability reported by this plugin that assigns users to the quarantine role.
8. In the **Instruction** text field, type the informational message that appears in the popup window to users if the plugin discovers a vulnerability.
9. In the **Link** field, type the URL where users can go to fix their systems. The URL appears as a link in the scan report. Make sure to enable traffic policies for the quarantine role to allow users HTTP access to the URL.
10. When finished, click **Update**.

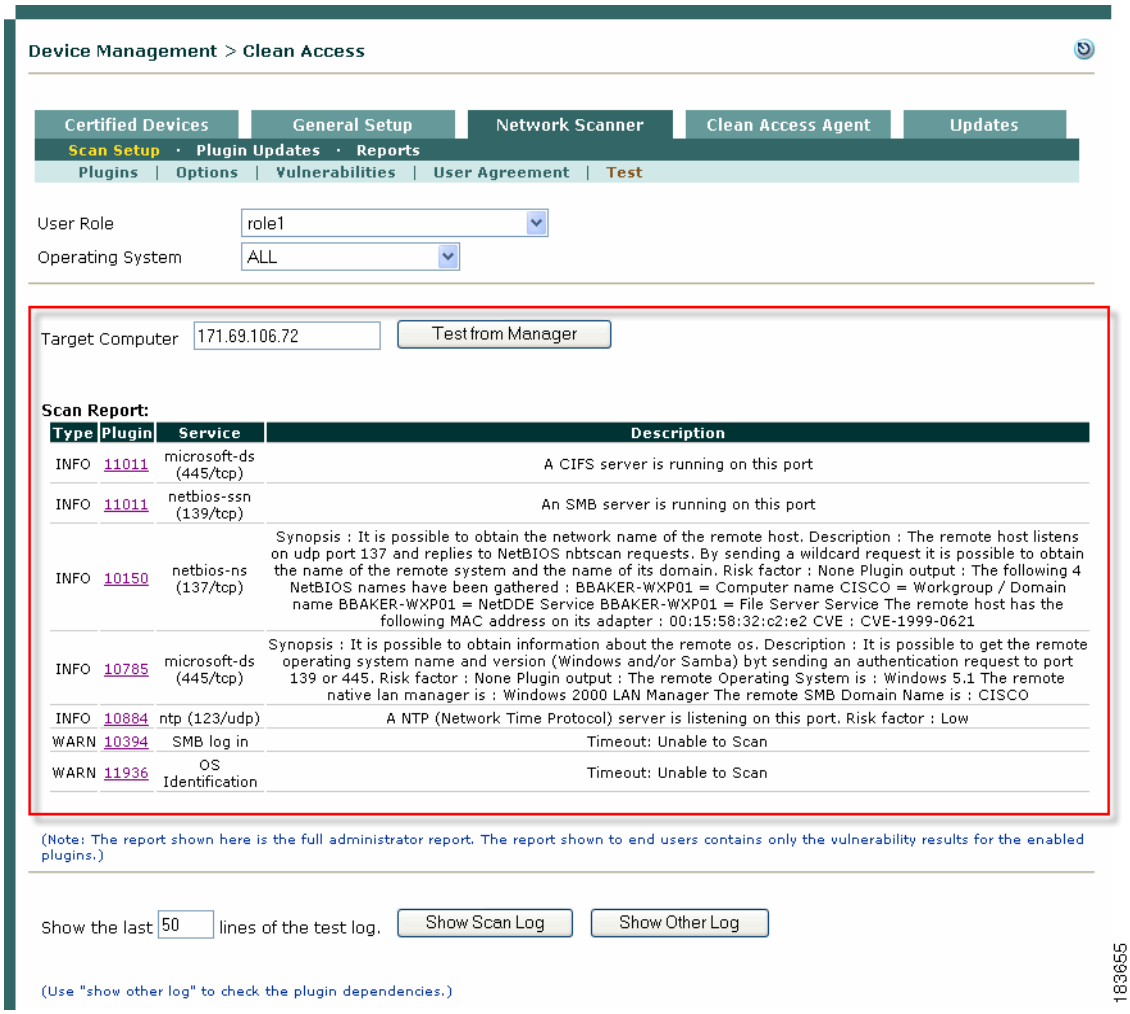
Test Scanning

The **Test** form lets you try out your scanning configuration. You can target any machine for the scan, and specify the user role to be assumed by the target client for the purpose of the test. For this type of testing, the test is actually performed against copies of the scan plugins that are kept in the Clean Access Manager. In a production environment, the Clean Access Servers get copies of scan plugins automatically from the Clean Access Manager and perform the scanning,

To perform a test scan:

1. Go to **Device Management > Clean Access > Network Scanner > Scan Setup > Test**.
2. Choose the **User Role** and **Operating System** for which you want to test the user.
3. Enter the IP address of the machine that you want to scan (the address of the current machine appears by default) in the **Target Computer** field.
4. Click **Test**. The scan result appears at the bottom of the page.

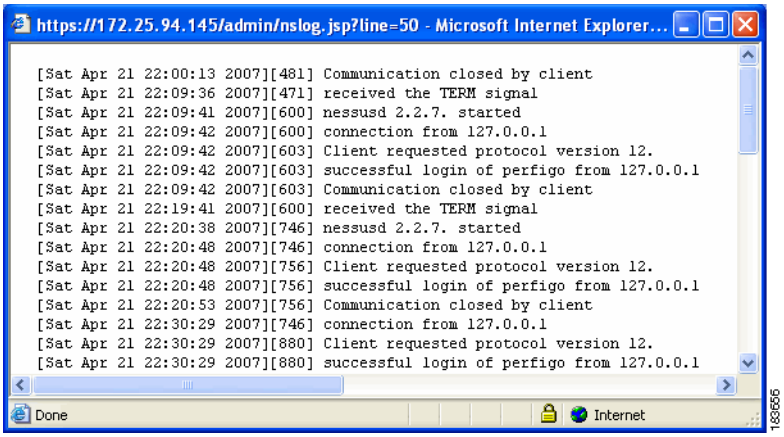
Figure 12-11 Network Scanning Test Page


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
User Role
role1
Operating System
ALL
Target Computer
171.69.106.72
Test from Manager
Scan Report:
Type Plugin Service Description
INFO 11011 microsoft-ds (445/tcp) A CIFS server is running on this port
INFO 11011 netbios-ssn (139/tcp) An SMB server is running on this port
INFO 10150 netbios-ns (137/tcp) Synopsis : It is possible to obtain the network name of the remote host. Description : The remote host listens on udp port 137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain. Risk factor : None Plugin output : The following 4 NetBIOS names have been gathered : BBAKER-WXP01 = Computer name CISCO = Workgroup / Domain name BBAKER-WXP01 = NetDDE Service BBAKER-WXP01 = File Server Service The remote host has the following MAC address on its adapter : 00:15:58:32:c2:e2 CVE : CVE-1999-0621
INFO 10785 microsoft-ds (445/tcp) Synopsis : It is possible to obtain information about the remote os. Description : It is possible to get the remote operating system name and version (Windows and/or Samba) byt sending an authentication request to port 139 or 445. Risk factor : None Plugin output : The remote Operating System is : Windows 5.1 The remote native lan manager is : Windows 2000 LAN Manager The remote SMB Domain Name is : CISCO
INFO 10884 ntp (123/udp) A NTP (Network Time Protocol) server is listening on this port. Risk factor : Low
WARN 10394 SMB log in Timeout: Unable to Scan
WARN 11936 OS Identification Timeout: Unable to Scan
(Note: The report shown here is the full administrator report. The report shown to end users contains only the vulnerability results for the enabled plugins.)
Show the last 50 lines of the test log.
Show Scan Log
Show Other Log
(Use "show other log" to check the plugin dependencies.)
183655

Show Log

Clicking the **Show Scan Log** button on the **Device Management > Network Scanner > Scan Setup > Test** page brings up a debug log (Figure 12-12) for the target computer tested (sourced from /var/nessus/logs/nessusd.messages). The log shows which plugins were executed, the results of the execution, which plugins were skipped and the reason (dependency, timeout, etc). Administrators can check this log to debug why a scan result is not as expected.

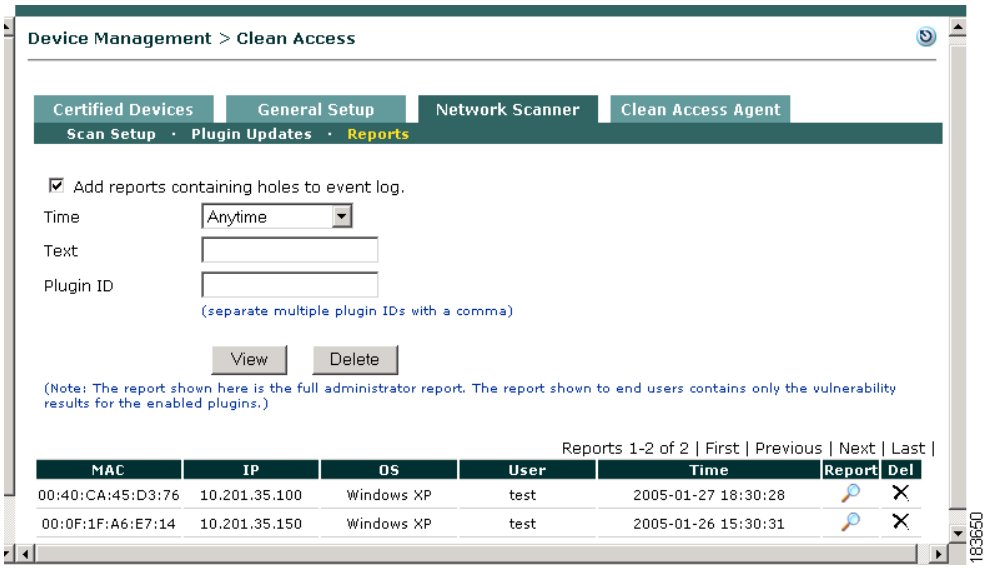
Figure 12-12 Network Scanning Show Log


https://172.25.94.145/admin/nslog.jsp?line=50 - Microsoft Internet Explorer...
[Sat Apr 21 22:00:13 2007][481] Communication closed by client
[Sat Apr 21 22:09:36 2007][471] received the TERM signal
[Sat Apr 21 22:09:41 2007][600] nessusd 2.2.7. started
[Sat Apr 21 22:09:42 2007][600] connection from 127.0.0.1
[Sat Apr 21 22:09:42 2007][603] Client requested protocol version 12.
[Sat Apr 21 22:09:42 2007][603] successful login of perfigo from 127.0.0.1
[Sat Apr 21 22:09:42 2007][603] Communication closed by client
[Sat Apr 21 22:19:41 2007][600] received the TERM signal
[Sat Apr 21 22:20:38 2007][746] nessusd 2.2.7. started
[Sat Apr 21 22:20:48 2007][746] connection from 127.0.0.1
[Sat Apr 21 22:20:48 2007][756] Client requested protocol version 12.
[Sat Apr 21 22:20:48 2007][756] successful login of perfigo from 127.0.0.1
[Sat Apr 21 22:20:53 2007][756] Communication closed by client
[Sat Apr 21 22:30:29 2007][746] connection from 127.0.0.1
[Sat Apr 21 22:30:29 2007][880] Client requested protocol version 12.
[Sat Apr 21 22:30:29 2007][880] successful login of perfigo from 127.0.0.1
Done
Internet
183656

View Scan Reports

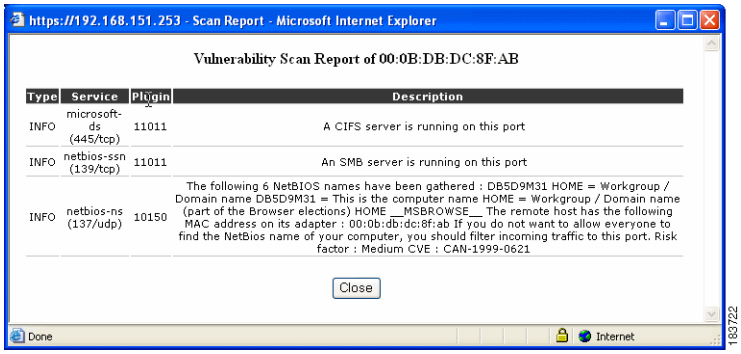
After enabling network scanning, you can view individual scan reports from **Device Management > Clean Access > Network Scanner > Reports**. The report shown here is the full administrator report (Figure 12-14). The report shown to end users contains only the vulnerability results for the enabled plugins. (Users can access their version of the scan report by clicking the **Scan Report** link in their Logout page.)

Figure 12-13 Network Scanner Reports



- Choose **Anytime** from the **Time** dropdown menu to view all reports.
- To view only selected reports, choose a different **Time**, or enter search **Text** or **Plugin ID**, and click **View**. If choosing a "**User Defined**" Time interval, type the "begin" year-month-day and time in the first text box (e.g. 2006-03-22 13:10:00) and the "end" year-month-day and time in the second text box (e.g.2006-03-23 11:25:00), then click **View**.
- To delete reports displayed according to the selected criteria, click **Delete**.
- Click the **Report** icon to open the detailed scan report, as shown in Figure 12-15.

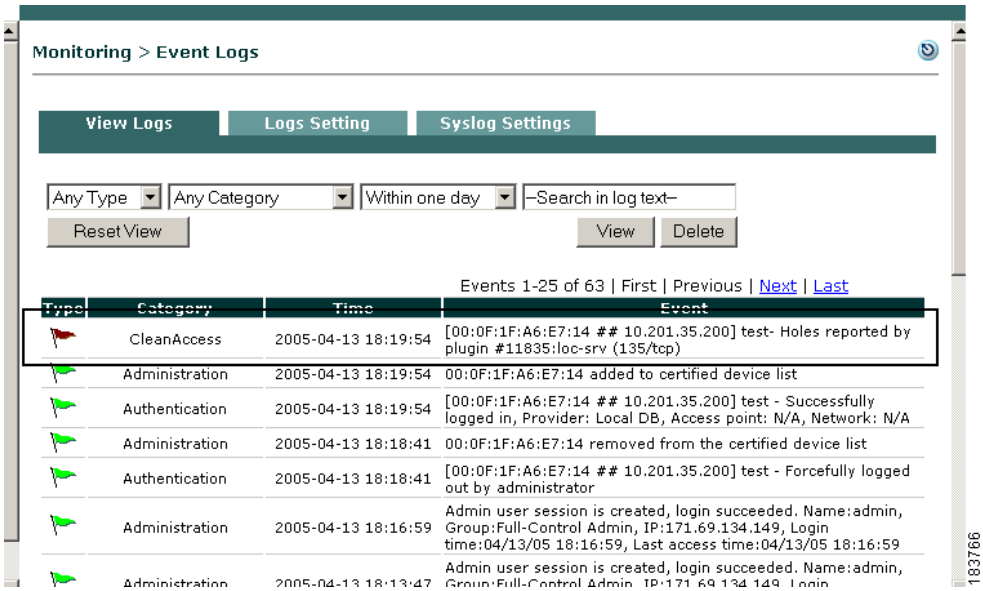
Figure 12-14 Network Scanner Administrator Report Example


https://192.168.151.253 - Scan Report - Microsoft Internet Explorer
Vulnerability Scan Report of 00:0B:DB:DC:8F:AB
Type
Service
Plugin
Description
INFO
microsoft-ds (445/tcp)
11011
A CIFS server is running on this port
INFO
netbios-ssn (139/tcp)
11011
An SMB server is running on this port
INFO
netbios-ns (137/udp)
10150
The following 6 NetBIOS names have been gathered : DB5D9M31 HOME = Workgroup / Domain name DB5D9M31 = This is the computer name HOME = Workgroup / Domain name (part of the Browser elections) HOME __MSBROWSE__ The remote host has the following MAC address on its adapter : 00:0b:db:dc:8f:ab If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. Risk factor : Medium CVE : CAN-1999-0621
Close
Done
Internet
183722

Note When there are dependencies between plugins, for example plugin B is enabled and the scan result of plugin A is the prerequisite of plugin B, the network scanner automatically applies plugin A whether or not plugin A is enabled. However, since plugin A is not explicitly enabled, the scan result reported from plugin A will only be shown in the administrator reports.

- To add reports to the Event log (**Monitoring > Event Logs > View Logs**), check the "**Add reports containing holes to event log"** option. CleanAccess category reports will be generated as shown in Figure 12-15.

Figure 12-15 CleanAccess Network Scanning Event Log



Customize the User Agreement Page

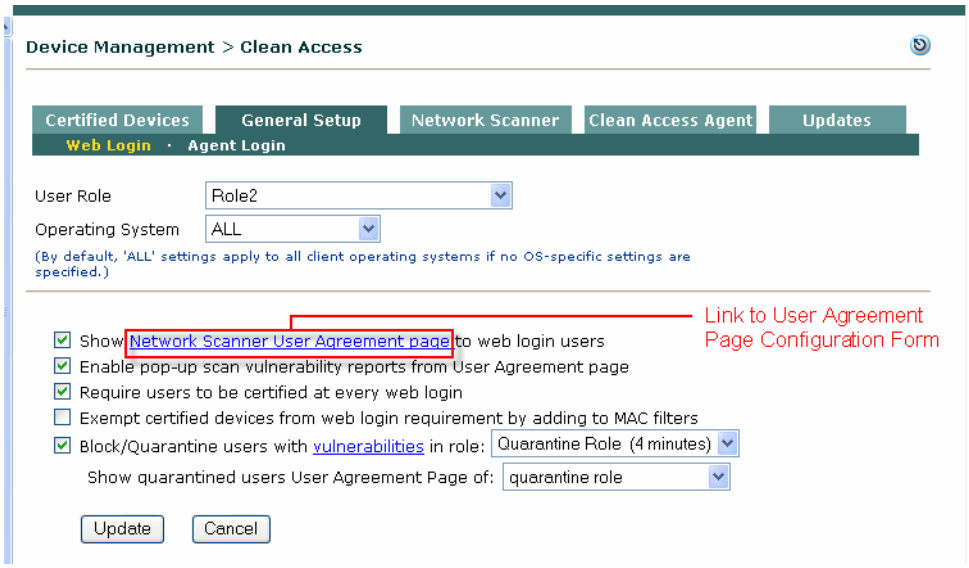
You can enable a User Agreement Page ("Virus Protection Page") for web login users to provide network usage policy information, virus warnings and/or links to software patches or updates after login and successful network scanning.

Only uncertified users will see the User Agreement Page. Once a user device is on the Certified Devices List, the User Agreement Page is not presented again until the device is cleared from the Certified Devices List. Note that the **Certified Devices List** only records the first user that logs in with the device and in this way tracks which user accepted the User Agreement Page at login. To ensure that the User Agreement Page is presented to users at each login, enable the **Require users to be certified at every web login** option for the role/OS on the **General Setup** page.

Configuration settings for this page are located in two places:

- The page target (whether the page is shown to users in a user role) is configured from **Device Management > Clean Access > General Setup** (Figure 12-16).

Figure 12-16 General Setup Tab


Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Web Login · Agent Login
User Role
Role2
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
Link to User Agreement Page Configuration Form
Show Network Scanner User Agreement page to web login users
Enable pop-up scan vulnerability reports from User Agreement page
Require users to be certified at every web login
Exempt certified devices from web login requirement by adding to MAC filters
Block/Quarantine users with vulnerabilities in role:
Quarantine Role (4 minutes)
Show quarantined users User Agreement Page of:
quarantine role
Update
Cancel
183648

- The page contents for a user role are configured under **Device Management Clean Access > Network Scanner > Scan Setup > User Agreement Page** (Figure 12-17).

Figure 12-17 User Agreement Page Content Configuration Form

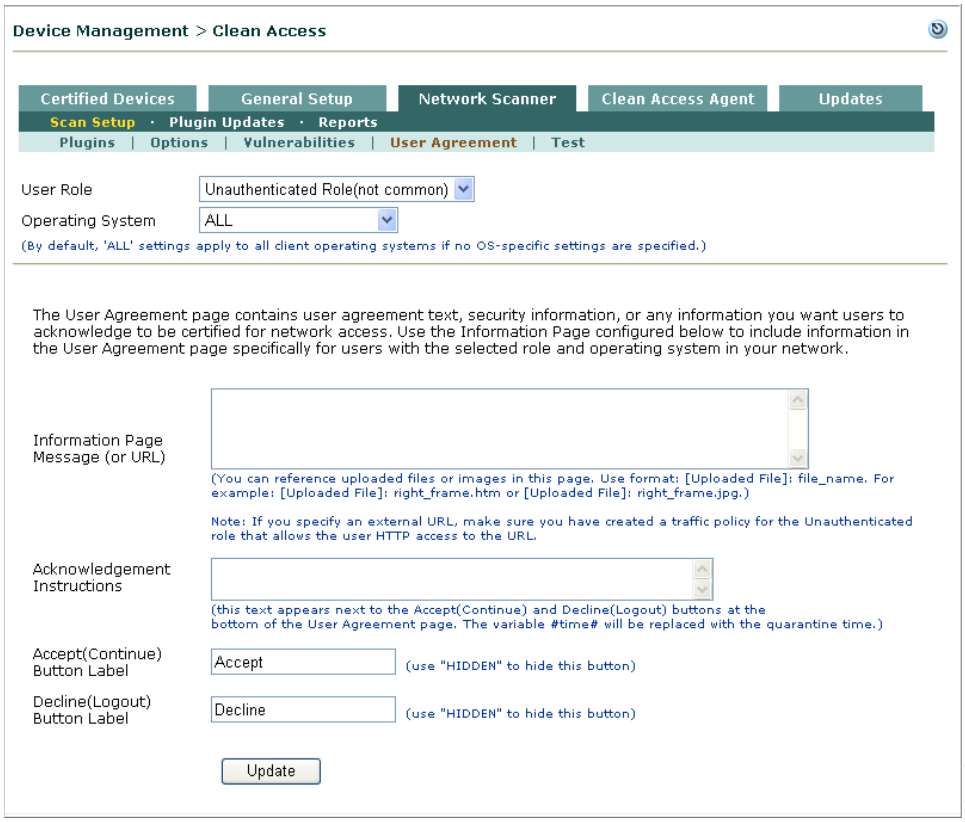
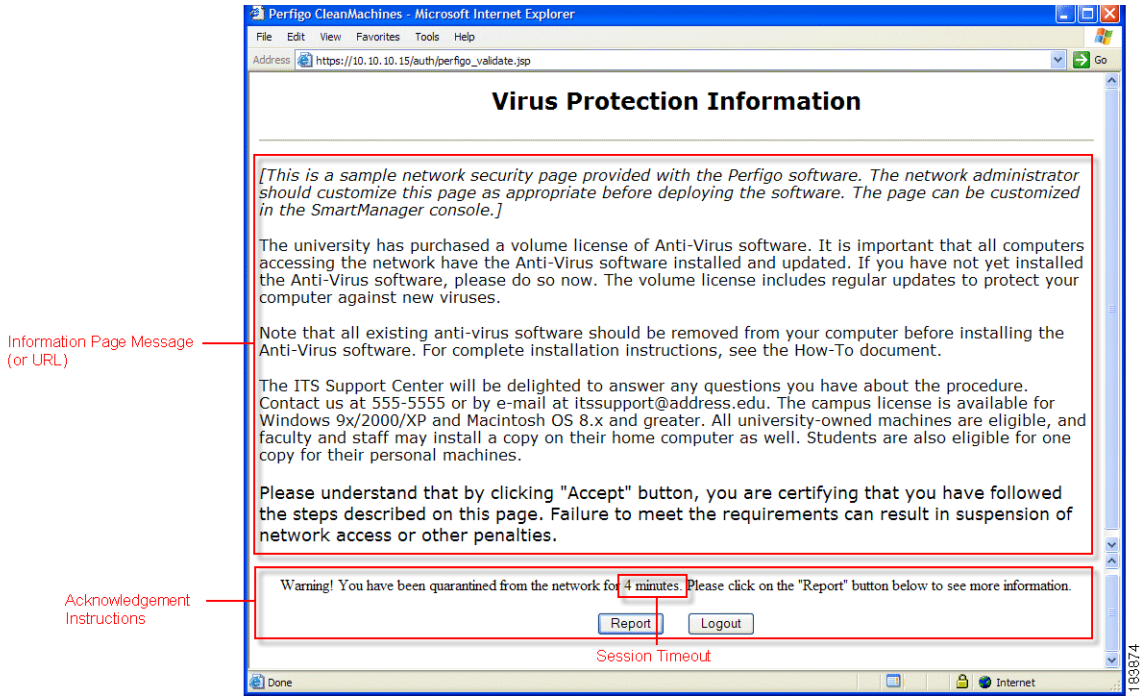

Device Management > Clean Access
Certified Devices
General Setup
Network Scanner
Clean Access Agent
Updates
Scan Setup · Plugin Updates · Reports
Plugins | Options | Vulnerabilities | User Agreement | Test
User Role
Unauthenticated Role(not common)
Operating System
ALL
(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)
The User Agreement page contains user agreement text, security information, or any information you want users to acknowledge to be certified for network access. Use the Information Page configured below to include information in the User Agreement page specifically for users with the selected role and operating system in your network.
Information Page Message (or URL)
(You can reference uploaded files or images in this page. Use format: [Uploaded File]: file_name. For example: [Uploaded File]: right_frame.htm or [Uploaded File]: right_frame.jpg.)
Note: If you specify an external URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access to the URL.
Acknowledgement Instructions
(this text appears next to the Accept(Continue) and Decline(Logout) buttons at the bottom of the User Agreement page. The variable #time# will be replaced with the quarantine time.)
Accept(Continue) Button Label
Accept
(use "HIDDEN" to hide this button)
Decline(Logout) Button Label
Decline
(use "HIDDEN" to hide this button)
Update
281778

Figure 12-18 illustrates what the default generated page looks like to an end user. The User Agreement Page is not a popup but an HTML frame-based page made up of several components:

- The **Information Page Message (or URL)** component, which contains the contents you specify.
- The **Acknowledgement Instructions** frame component. This contains text and buttons (Accept, Decline) for acknowledging the agreement information.

Note For quarantine role pages, the buttons are hardcoded to read “Report” and “Logout”.

Figure 12-18 User Agreement Page (Quarantine Role Example)


Perfigo CleanMachines - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.10.10.15/auth/perfigo_validate.jsp
Go
Virus Protection Information
[This is a sample network security page provided with the Perfigo software. The network administrator should customize this page as appropriate before deploying the software. The page can be customized in the SmartManager console.]
The university has purchased a volume license of Anti-Virus software. It is important that all computers accessing the network have the Anti-Virus software installed and updated. If you have not yet installed the Anti-Virus software, please do so now. The volume license includes regular updates to protect your computer against new viruses.
Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.
The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact us at 555-5555 or by e-mail at itssupport@address.edu. The campus license is available for Windows 9x/2000/XP and Macintosh OS 8.x and greater. All university-owned machines are eligible, and faculty and staff may install a copy on their home computer as well. Students are also eligible for one copy for their personal machines.
Please understand that by clicking "Accept" button, you are certifying that you have followed the steps described on this page. Failure to meet the requirements can result in suspension of network access or other penalties.
Warning! You have been quarantined from the network for 4 minutes. Please click on the "Report" button below to see more information.
Report
Logout
Done
Internet
Information Page Message (or URL)
Acknowledgement Instructions
Session Timeout
183874

Note The page content ("Virus Protection Information") shown in Figure 12-18 is the default content shown to the end user, if no other information message or URL is specified for the User Agreement Page. Note that this default content is not displayed in the **Information Page Message (or URL)** text area of the configuration form.

The configuration form (shown in Figure 12-17) can be used to set up the following types of pages for a web login user:

- After network scanning with no system vulnerabilities found—Users see the User Agreement Page configured for the normal login role (Accept and Decline buttons).
- After web login and network scanning with client system vulnerabilities found—
  - Users are put in a quarantine role and see the User Agreement Page of the quarantine role (**Report** and **Logout** buttons).
  - Users are put in a quarantine role but see the User Agreement Page of their normal login role (**Report** and **Logout** buttons).

Before starting, create the HTML page that you want to use for the **Information Page Message (or URL)** component. Cisco NAC Appliance lets you present a specific information page to users with a particular role or operating system. The customized page should be on a web server accessible to Cisco NAC Appliance elements.

After configuring the User Agreement Page, you will need to create a traffic policy to enable users in the role access to the web resources of the page. Note that the role must grant access to port 80 of the CAM. See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" for details.

To customize the User Agreement Page:

1. Go to **Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement Page**. The configuration form for the User Agreement Page appears as shown in Figure 12-17.

2. Choose the **User Role** and **Operating System** for which the page applies. The Clean Access Manager determines the operating system of the user's system at login time and serves the page you have specified for that operating system. If selecting a quarantine role, the **Acknowledgement Instructions** and button fields will be disabled.
3. Type HTML content or the URL of the page that you want to appear in the **Information Page Message (or URL)** field of the User Agreement page. If using a file you uploaded to the CAM or CAS, you can reference the file as described below:
   a. ***Enter URLs:*** (for a single webpage to appear)

      For an external URL, use the format `http://www.webpage.com`.

      For a URL on the CAM use the format:

      ```
      [Uploaded File]:file_name.htm
      ```

      For images, use the format:

      ```
      [Uploaded File]:file_name.jpg
      ```

Note If you enter an external URL or CAM URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access only to the CAM or external server.

   b. ***Enter HTML:*** (to add a combination of resource files, such as logos and HTML links)

      Type HTML content directly into the text field.

      To reference an uploaded resource file as part of the HTML content, use the following formats:

      - To reference a link to an uploaded HTML file:

        ```
        <a href="file_name.html"> file_name.html </a>
        ```

      - To reference an image file (such as a JPEG file) enter:

        ```
        <img src="file_name.jpg">
        ```

      See Upload a Resource File, page 5-13 for additional details.
4. If desired, type the text that you want to appear above the accept and decline buttons in the **Acknowledgement Instructions** field.
5. Type the labels that should appear on the accept and decline buttons in their respective fields.
6. Click the **Save** button to save your changes.

The User Agreement Page is now generated with the changes you made for users logging into the network.

Note For details on the web user login page, see Chapter 5, "Configuring User Login Page and Guest Access." For traffic policy details, see Configure Policies for Agent Temporary and Quarantine Roles, page 8-19.



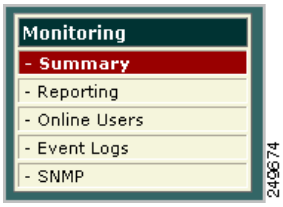
Monitoring Event Logs

This chapter describes the Monitoring module of Cisco NAC Appliance. Topics include:

- Overview, page 13-1
- Interpreting Event Logs, page 13-4
- Configuring Syslog Logging, page 13-9
- Cisco NAC Appliance Log Files, page 13-11
- SNMP, page 13-12

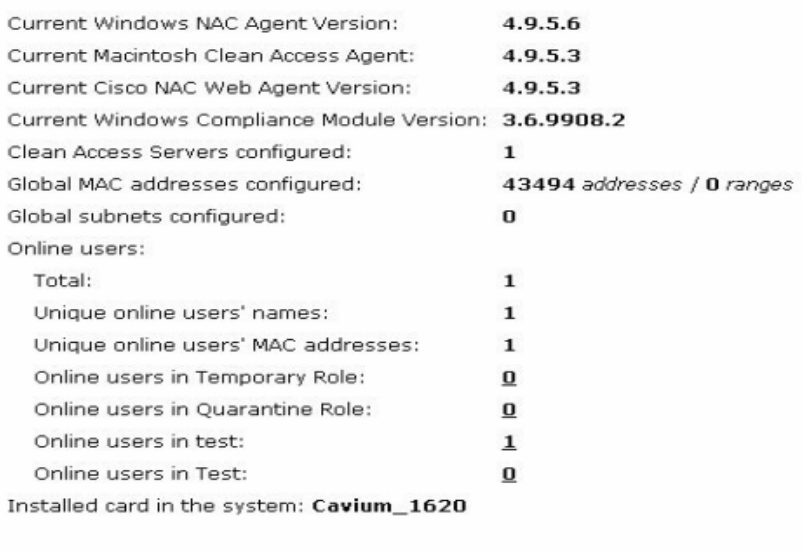
Overview

Figure 13-1 Monitoring Module



The Monitoring pages provide operational information for your deployment, including information on user activity, syslog events, network configuration changes. The Monitoring module also provides basic SNMP polling and alerts. The Monitoring Summary status page summarizes several important statistics, shown in Figure 13-2.

Figure 13-2 Monitoring > Summary Page


Current Windows NAC Agent Version: 4.9.5.6
Current Macintosh Clean Access Agent: 4.9.5.3
Current Cisco NAC Web Agent Version: 4.9.5.3
Current Windows Compliance Module Version: 3.6.9908.2
Clean Access Servers configured: 1
Global MAC addresses configured: 43494 addresses / 0 ranges
Global subnets configured: 0
Online users:
Total: 1
Unique online users' names: 1
Unique online users' MAC addresses: 1
Online users in Temporary Role: 0
Online users in Quarantine Role: 0
Online users in test: 1
Online users in Test: 0
Installed card in the system: Cavium_1620

The page includes the information shown in Table 13-1.

Table 13-1 Monitoring > Summary Page

Item	Description
Current Windows NAC Agent Version	The current Windows version of the Agent installed with the CAM software or manually uploaded (reflects the contents of the **Version** field).
Current Macintosh Clean Access Agent	The current version of the Mac OS X Cisco NAC Agent installed with the CAM software or manually uploaded (reflects the contents of the **Version** field).
Current Cisco NAC Web Agent Version	The current version of the Cisco NAC Web Agent installed with the CAM software or manually uploaded (reflects the contents of the **Version** field).
Clean Access Servers configured	The number of Clean Access Servers configured in the CAS management pages for the Clean Access Manager domain.
Global MAC addresses configured (addresses/ranges)	The number of addresses and ranges currently in the MAC/IP device filter passthrough list. For details on MAC passthrough lists, see Global Device and Subnet Filtering, page 2-10.
Global Subnets configured	The number of subnet addresses currently in the subnet-based passthrough list. For more information, see Global Device and Subnet Filtering, page 2-10.

Table 13-1 Monitoring > Summary Page (continued)

Item	Description
Online users (In-Band / Out-of-Band)	These entries list: • Total number of IB and/or OOB online user names • Total number of IB and/or OOB online MAC addresses • Number of IB and OOB online users per user role **Note** Per-role user tallies are links to the **Monitoring > Online Users > View Online Users** page. Clicking a link displays the IB or OOB online user list for the particular role. For more information, see Online Users list, page 11-28.
Installed card in the system	Indicates one or both of the following: • For non-FIPS NAC-3140, 3310, 3350, and 3390 appliances—whether or not a Cavium accelerator card (like the Cavium 1120) is installed in the appliance. • For FIPS 140-2 compliant NAC-3310, 3350, and 3390 (appliances into which you have installed a field-replaceable FIPS card)—whether a FIPS card is installed and enabled on the system to provide FIPS compliant functions for your deployment and whether or not the System is running in FIPS mode. • For FIPS 140-2 compliant next generation appliances (NAC-3315, 3355, and 3395)—whether a FIPS card is installed and enabled on the system to provide FIPS compliant functions for your deployment and whether or not the System is running in FIPS mode.

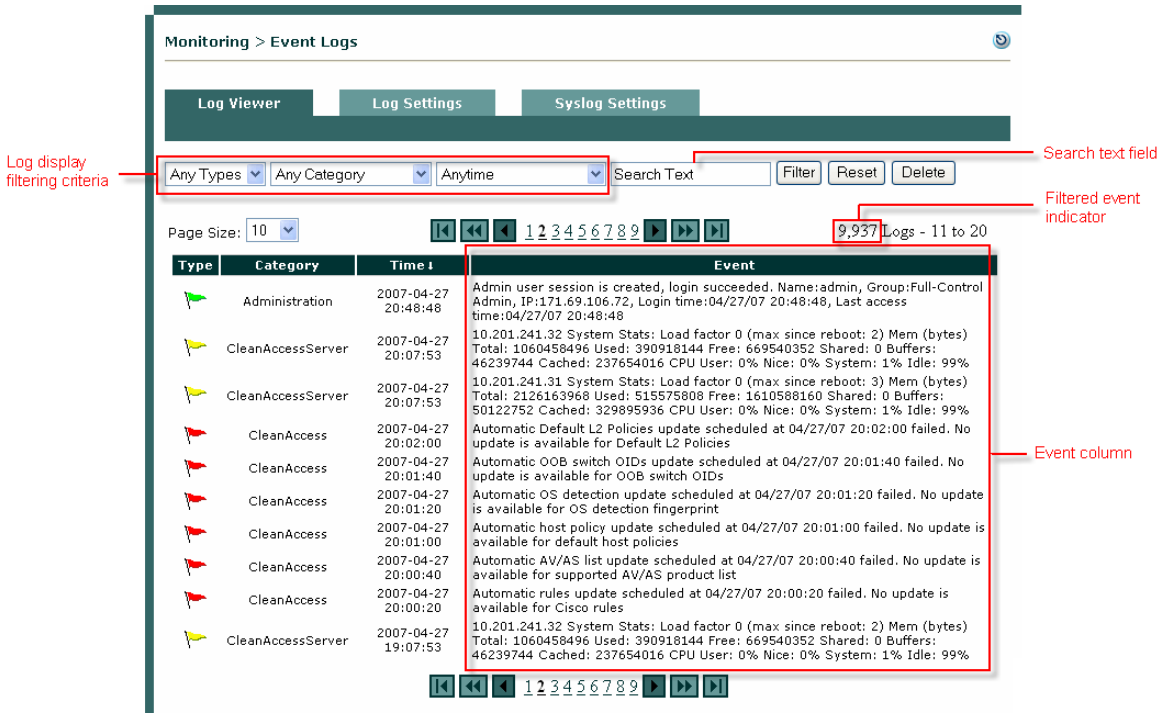
Interpreting Event Logs

Click the **Event Logs** link in the **Monitoring** module to view syslog-based event logs in the admin console. There are three Event Logs tabs: **Log Viewer**, **Logs Settings**, and **Syslog Settings**.

View Logs

Figure 13-3 shows the Log Viewer pane.

Figure 13-3 Log Viewer Pane


Monitoring > Event Logs
Log Viewer
Log Settings
Syslog Settings
Log display filtering criteria
Any Types
Any Category
Anytime
Search Text
Filter
Reset
Delete
Search text field
Filtered event indicator
Page Size: 10
1 2 3 4 5 6 7 8 9
9,937 Logs - 11 to 20
Type
Category
Time
Event
Administration
2007-04-27 20:48:48
Admin user session is created, login succeeded. Name:admin, Group:Full-Control Admin, IP:171.69.106.72, Login time:04/27/07 20:48:48, Last access time:04/27/07 20:48:48
CleanAccessServer
2007-04-27 20:07:53
10.201.241.32 System Stats: Load factor 0 (max since reboot: 2) Mem (bytes) Total: 1060458496 Used: 390918144 Free: 669540352 Shared: 0 Buffers: 46239744 Cached: 237654016 CPU User: 0% Nice: 0% System: 1% Idle: 99%
CleanAccessServer
2007-04-27 20:07:53
10.201.241.31 System Stats: Load factor 0 (max since reboot: 3) Mem (bytes) Total: 2126163968 Used: 515575808 Free: 1610588160 Shared: 0 Buffers: 50122752 Cached: 329895936 CPU User: 0% Nice: 0% System: 1% Idle: 99%
CleanAccess
2007-04-27 20:02:00
Automatic Default L2 Policies update scheduled at 04/27/07 20:02:00 failed. No update is available for Default L2 Policies
CleanAccess
2007-04-27 20:01:40
Automatic OOB switch OIDs update scheduled at 04/27/07 20:01:40 failed. No update is available for OOB switch OIDs
CleanAccess
2007-04-27 20:01:20
Automatic OS detection update scheduled at 04/27/07 20:01:20 failed. No update is available for OS detection fingerprint
CleanAccess
2007-04-27 20:01:00
Automatic host policy update scheduled at 04/27/07 20:01:00 failed. No update is available for default host policies
CleanAccess
2007-04-27 20:00:40
Automatic AV/AS list update scheduled at 04/27/07 20:00:40 failed. No update is available for supported AV/AS product list
CleanAccess
2007-04-27 20:00:20
Automatic rules update scheduled at 04/27/07 20:00:20 failed. No update is available for Cisco rules
CleanAccessServer
2007-04-27 19:07:53
10.201.241.32 System Stats: Load factor 0 (max since reboot: 2) Mem (bytes) Total: 1060458496 Used: 390918144 Free: 669540352 Shared: 0 Buffers: 46239744 Cached: 237654016 CPU User: 0% Nice: 0% System: 1% Idle: 99%
Event column
183765

The **Log Viewer** tab includes the following information:

- System statistics for Clean Access Servers (generated every hour by default)
- User activity, with user logon times, log-off times, failed logon attempts, and more.
- Network configuration events, including changes to the MAC or IP passthrough lists, and addition or removal of Clean Access Servers.
- Device management events (for OOB), including when linkdown traps are received, and when a port changes to the Auth or Access VLAN.
- Changes or updates to Cisco NAC Appliance checks, rules, and Supported AV/AS Product List.
- Changes to Clean Access Server DHCP configuration.

System statistics are generated for each CAS managed by the Clean Access Manager every hour by default. See Configuring Syslog Logging, page 13-9 to change how often system checks occur.

Note The most recent events appear first in the Events column.

Table 13-2 describes the navigation, searching capabilities, and actual syslog displayed on the Log Viewer page.

Table 13-2 Log Viewer Page

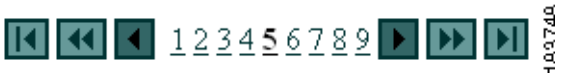
	Column	Description
Navigation	**First Page/Previous Page/ Previous Entry/Specific Page/Next Entry/Next Page/Last Page**	These navigation links page through the event log. The most recent events appear first in the Events column. The **Last** link shows you the oldest events in the log. 
	Page Size	The number of log entries displayed in the window. (You can specify 10, 25, or 100 entries per page.)
	Column	Click a column heading (e.g. Type or Category) to sort the Event log by that column.

Table 13-2 Log Viewer Page (continued)

	Column	Description
Search criteria	**Type**	Search by Type column criteria (then click **Filter**): • Any Type • Failure • Information • Success
	Category	Search by Category column criteria (then click **Filter**): • Authentication [1] • Administration • Client • Clean Access Server • Clean Access • SW_Management (if OOB is enabled) • DHCP • Guest Registration • SSL Communication • Miscellaneous
	Time	Search by the following Time criteria (then click **Filter**): • Within one hour • Within one day • Within two days • Within one week • Anytime • One hour ago • One day ago • Two days ago • One week ago
	Search in log text	Type desired search text and click **Filter**
Controls	**Filter**	After selecting the desired search criteria, click **Filter** to display the results.
	Reset	Clicking **Reset** restores the default view, in which logs within one day are displayed.
	Delete	Clicking Delete removes the events filtered through the search criteria across the number of applicable pages. Clicking Delete removes filtered events from Clean Access Manager storage. Otherwise, the event log persists through system shutdown. Use the filter event indicator shown in Figure 13-3 on page 13-4 to view the total number of filtered events that are subject to being deleted.

Table 13-2 Log Viewer Page (continued)

	Column	Description
Status Display	**Type**	• Red flag ( ) = Failure; indicates error or otherwise unexpected event. • Green flag ( ) = Success; indicates successful or normal usage event, such as successful login and configuration activity. • Yellow flag ( ) = Information; indicates system performance information, such as load information and memory usage.
	Category	Indicates the module or system component that initiated the log event. (For a list, see Category, page 13-6.) Note that system statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default.
	Time	Displays the date and time (hh:mm:ss) of the event, with the most recent events appearing first in the list.
	Event	Displays the event for the module, with the most recent events listed first. See Table 13-3 on page 13-7 for an example of Clean Access Server event.

1. Authentication-type entries may include the item "Provider: <provider type>, Access point: N/A, Network: N/A." To continue to provide support for the EOL'ed legacy wireless client (if present and pre-configured in the Manager), the "Access point: N/A, Network: N/A" fields provide AP MAC and SSID information respectively for the legacy client.

Event Log Example

Table 13-3 explains the following typical Clean Access Server health event example:

```
CleanAccessServer 2007-04-05 09:03:31 10.201.15.2 System Stats: Load factor 0 (max
since reboot: 2) Mem (bytes) Total: 528162816 Used: 295370752 Free: 232792064 Shared:
0 Buffers: 41537536 Cached: 179576832 CPU User: 0% Nice: 0% System: 1% Idle: 99%
```

Table 13-3 Event Column Fields

Value	Description
`CleanAccessServer`	A Clean Access Server is reporting the event
2007-04-05 09:03:31	Date and time of the event
10.201.15.2	IP address of reporting Clean Access Server
`System Stats:`	System statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default.
`Load factor 0`	Load factor is a number that describes the number of packets waiting to be processed by the Clean Access Server (that is, the current load being handled by the CAS). When the load factor grows, it is an indication that packets are waiting in the queue to be processed. If the load factor exceeds 500 for any consistent period of time (e.g. 5 minutes), this indicates that the Clean Access Server has a steady high load of incoming traffic/packets. You should be concerned if this number increases to 500 or above.
`(max since reboot: <n>)`	The maximum number of packets in the queue at any one time (i.e. the maximum load handled by the Clean Access Server).

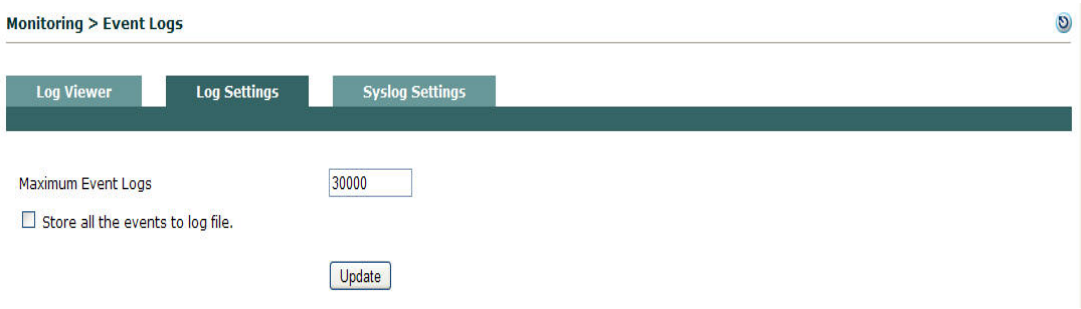
Table 13-3 Event Column Fields (continued)

Value	Description
Mem Total: 528162816 bytes	These are the memory usage statistics. There are 6 numbers shown here: total memory, used memory, free memory, shared memory, buffer memory, and cached memory.
Used: 295370752 bytes	
Free: 232792064 bytes	
Shared: 0 bytes	
Buffers: 41537536 bytes	
Cached: 179576832 bytes	
CPU User: 0%	These numbers indicate CPU processor load on the hardware, in percentages. These four numbers indicate time spent by the system in user, nice, system, and idle processes. **Note** Time spent by the CPU in system process is typically < 90% on a Clean Access Server. This indicates a healthy system.
Nice: 0%	
System: 1%	
Idle: 99%	

Limiting the Number of Logged Events

The event log threshold is the number of events to be stored in the Clean Access Manager database. The maximum number of log events kept on the CAM, by default, is 100,000. You can specify an event log threshold of up to 200,000 entries to be stored in the CAM database at a time. The event log is a circular log. The oldest entries will be overwritten when the log passes the event log threshold.

Table 13-4 Log Settings



To change the maximum number of events:

1. Click the **Logs Setting** tab in the **Monitoring > Event Logs** pages.
2. Type the new number in the **Maximum Event Logs** fields.
3. Enable **Store all the events to log file** checkbox to store all events to the **nac_manager.log** file.
4. Click **Update**.

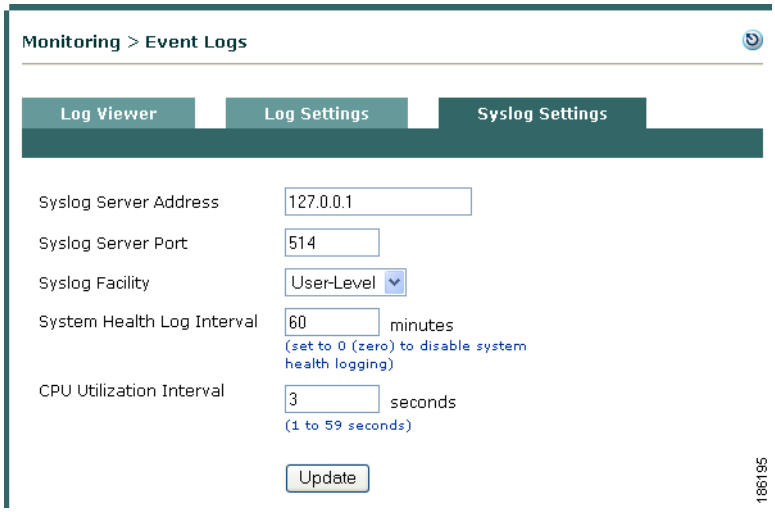
Configuring Syslog Logging

System statistics are generated for each Clean Access Server managed by the Clean Access Manager every hour by default. By default, event logs are written to the CAM. You can redirect CAM event logs to another server (such as your own syslog server).

Additionally, you can configure how often you want the CAM to log system status information by setting the value in the **Syslog Health Log Interval** field (default is **60** minutes).

To configure Syslog logging:

Step 1 Go to **Monitoring > Event Logs > Syslog Settings**.



Step 2 In the **Syslog Server Address** field, type the IP address of the Syslog server (default is **127.0.0.1**).

Note Multiple IP Addresses are not accepted.

Step 3 In the **Syslog Server Port** field, type the port for the Syslog server (default is **514**).

Step 4 Specify a **Syslog Facility** from the dropdown list. This setting enables you to optionally specify a different Syslog facility type for Syslog messages originating from the CAM. You can use the default "User-Level" facility type, or you can assign any of the "local use" Syslog facility types defined in the Syslog RFC ("Local use 0" to "Local use 7"). This feature gives you the ability to differentiate Cisco NAC Appliance Syslog messages from other "User-Level" Syslog entries you may already generate and direct to your Syslog server from other network components.

Step 5 In the **System Health Log Interval** field, specify how often you want the CAM to log system status information, in minutes (default is **60** minutes). This setting determines how frequently CAS statistics are logged in the event log.

Step 6 In the **CPU Utilization Interval** field, specify how often, in seconds, you want the CAM to record CPU utilization statistics. You can configure the CAM to record CPU status information up to nearly every minute and the default is every **3** seconds.

Step 7 Click the **Update** button to save your changes.

Note After you set up your Syslog server in the CAM, you can test your configuration by logging off and logging back into the CAM admin console. This will generate a Syslog event. If the CAM event is not seen on your Syslog server, make sure that the Syslog server is receiving UDP 514 packets and that they are not being blocked elsewhere on your network.

Note You can only forward to one syslog server. You can have that syslog server forward to another if required.

Cisco NAC Appliance Log Files

Table 13-5 lists common Clean Access Manager and Clean Access Server logs in Cisco NAC Appliance.

Table 13-5 Cisco NAC Appliance Log Files

File	Description
/var/log/messages	Startup
/perfigo/control/tomcat/logs/nac_manager.log	Perfigo service logs for release 4.5 and later [1,2]
/perfigo/control/data/details.html /perfigo/control/data/upgrade.html	CAM upgrade logs
/var/nessus/logs/nessusd.messages	Nessus plugin test logs
/perfigo/control/apache/logs/*	SSL (certificates), Apache error logs
/perfigo/control/tomcat/logs/catalina.out	Tomcat initialization logs
/var/log/ha-log	High availability logs (both CAM and CAS)
/var/log/dhcplog	DHCP relay, DHCP logs (CAS)
/perfigo/access/data/details.html /perfigo/access/data/upgrade.html	CAS upgrade logs
/perfigo/access/tomcat/logs/nac_server.log	Certificate-related CAM/CAS connection errors (CAS)

1. Device Management events for notifications received by the CAM from switches are written only to the logs on the file system (**/perfigo/control/tomcat/logs/nac_manager.log**). These events are written to disk only when the log level is set to INFO or finer.
2. Perfigo service log files in previous releases of Cisco NAC Appliance reside in the **/perfigo/logs/perfigo-log0.log.*** or **/tmp/perfigo-log0.log.*** (pre-release 3.5(5)) directory. For these older logs, 0 instead of * shows the most recent log.

Log File Sizes

- There are 10 logs with a maximum size of 20 MB for the **/perfigo/control/tomcat/logs/nac_manager.log** log file.
- There are 20 logs with maximum size of 20 MB for each log file under **/perfigo/(control | access)/apache/logs**.

The log file sizes can be controlled by using the following files:

- On Clean Access Manager, logging is controlled by the file: **/perfigo/control/tomcat/conf/logback.xml**
- On Clean Access Server, logging is controlled by the file: **/perfigo/access/tomcat/conf/logback.xml**

In the above xml files, the following parameters can be changed to control the log file size:

- **<MinIndex>** — Determines the minimum index of the log file name extension.
- **<MaxIndex>** —Determines the maximum index of the extension.

The difference between the above two parameters determines the count of files.

- **<MaxFileSize>** — Determines the file size limit of each log file.

The command **ls -clt** lists the log files available.

Note Cisco recommends to increase the count and limit moderately.

Note Use **service perfigo restart** to pickup the new logging configuration.

For additional details see also:

- Support Logs, page 14-42
- Certificate-Related Files, page 14-24.
- Backing Up the CAM Database, page 14-58

SNMP

You can configure the Clean Access Manager to be managed/monitored by an SNMP management tool (such as HP OpenView). This feature provides minimal manageability using SNMP (v1).

You can configure the Clean Access Manager for basic SNMP polling and alerting through **Monitoring > SNMP**. Note that SNMP polling and alerts are disabled by default.

Clicking the **Enable** button preceding **SNMP on NAC Manager** under **Monitoring > SNMP** activates the following features:

- SNMP Polling—If an SNMP `rocommunity` ("Read-only community") string is specified, the Clean Access Manager will respond to `snmpget` and `snmpwalk` requests with the correct community string.
- SNMP Traps—The Clean Access Manager can be configured to send traps by adding trap sinks. A *trap sink* is any computer configured to receive traps, typically a management box. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

When enabled, the SNMP module monitors the following processes:

- SSH Daemon
- Postgres Database
- Clean Access Manager
- Apache Web Server

The Clean Access Manager also sends traps in the following cases:

- When the Clean Access Manager comes online.
- When the Clean Access Manager shuts down.
- When the Clean Access Manager gains or loses contact with any Clean Access Servers it manages.
- When the SNMP service starts (a Cold Start Trap is sent).

Starting from Cisco NAC Appliance Release 4.9, you can configure the Clean Access Server to be managed/monitored by the SNMP management tool as well. Clicking the **Enable** button preceding **SNMP on NAC Servers** under **Monitoring > SNMP** activates the following features:

- SNMP Polling—If an SNMP `rocommunity` ("Read-only community") string is specified, the Clean Access Server will respond to `snmpget` and `snmpwalk` requests with the correct community string.

- SNMP Traps—The Clean Access Servers can be configured to send traps by adding trap sinks. A *trap sink* is any computer configured to receive traps, typically a management box. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

When enabled, the SNMP module monitors the following processes:

- SSH Daemon
- Java Process
- Apache Web Server process
- Clean Access Server

The Clean Access Server also sends traps in the following cases:

- When Clean Access Server shuts down.
- When Clean Access Server becomes Active.
- When Clean Access Server becomes Standby.
- When there is Linkup and Linkdown of interfaces.
- When disk utilization crosses the threshold.
- When the SNMP service starts (a Cold Start Trap is sent).
- When the swap partition free space falls below the threshold.

Note When management VLAN is set for CAS Eth0 interface, the SNMP management for CAS is not supported. In Virtual Gateway mode, it is mandatory to set the management VLAN. Hence SNMP management for CAS is not supported in the Virtual Gateway mode.

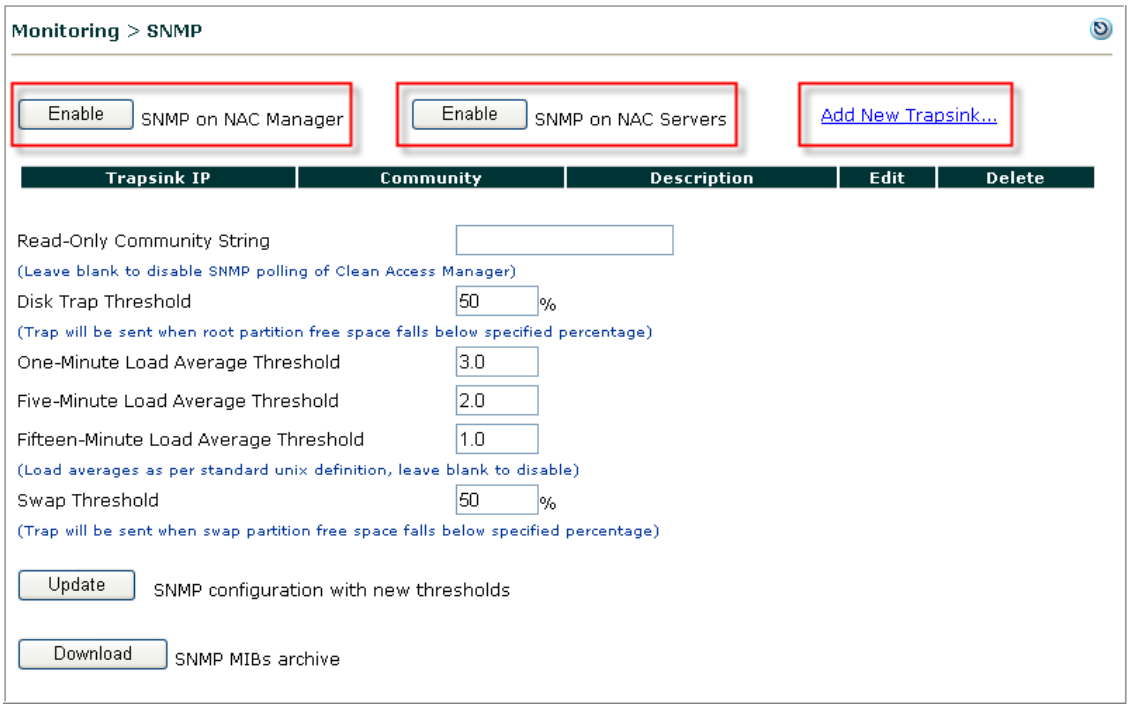
This section describes the following:

- Enable SNMP Polling/Alerts, page 13-13
- Add New Trapsink, page 13-15

Enable SNMP Polling/Alerts

Step 1 Go to **Monitoring > SNMP** to bring up the SNMP configuration page (Figure 13-4).

Figure 13-4 Monitoring > SNMP Page



Step 2 Click the **Enable** button preceding **SNMP on NAC Manager** to activate SNMP polling and SNMP traps in the Clean Access Manager.

Step 3 Click the **Enable** button preceding **SNMP on NAC Servers** to activate the SNMP polling and SNMP traps in all the Clean Access Servers connected to the Clean Access Manager.

Step 4 Specify values for the following fields:

- **Read-Only Community String:**
  Specify a string to enable the Clean Access Manager to respond to snmpget and snmpwalk requests with the correct community string. Leave this field blank to disable all Clean Access Manager responses to SNMP polling of the Clean Access Manager.
- **Disk Trap Threshold%:** (default is 50%)
  A trap will be sent when root partition free space falls below specified percentage.
- **One-Minute Load Average Threshold:** (default is 3.0)
  A trap will be sent when the one-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
- **Five-Minute Load Average Threshold:** (default is 2.0)
  A trap will be sent when the 5-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
- **Fifteen-Minute Load Average Threshold:** (default is 1.0)
  A trap will be sent when the 15-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
- **Swap Threshold:** (default is 50%)
  A trap will be sent when swap partition free space falls below specified percentage.

Step 5 Click **Update** to update the SNMP configuration with new thresholds.

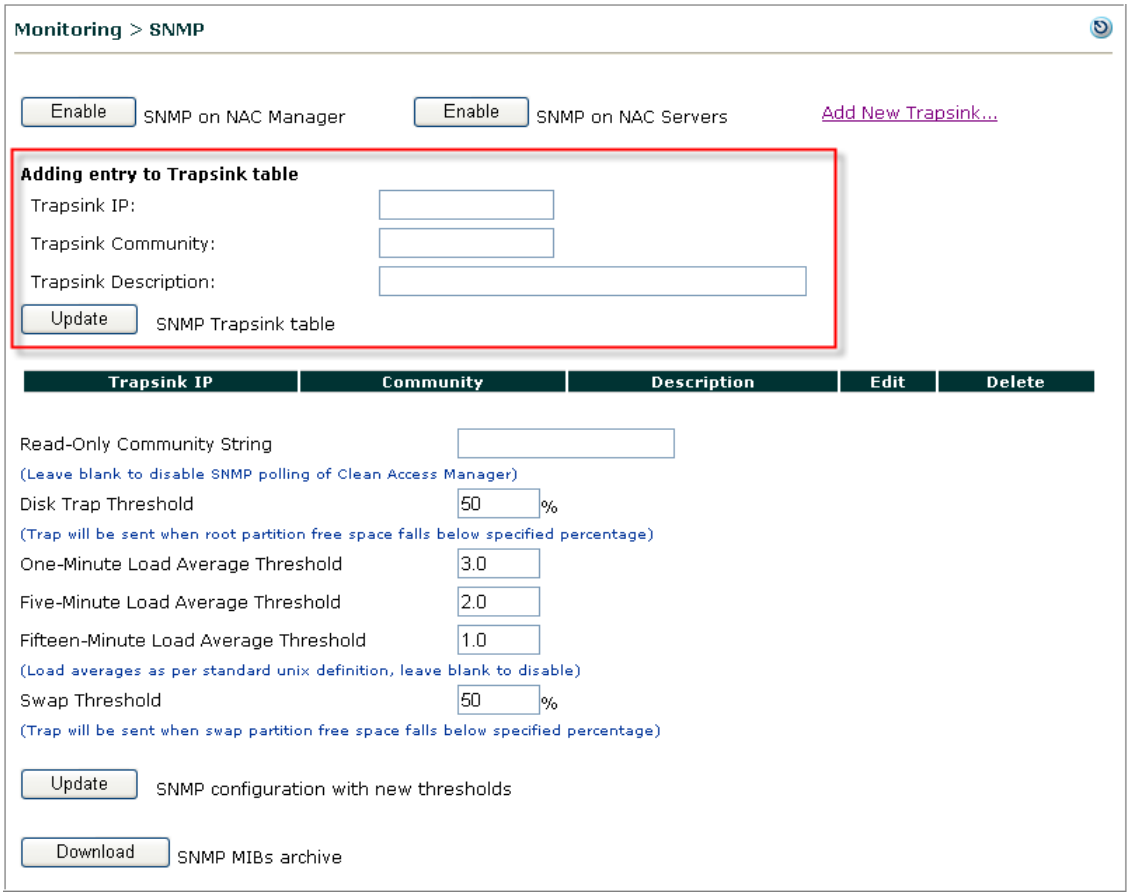
Step 6 Click **Download** to download the SNMP MIB archive in .tar.gz form.

Add New Trapsink

The Clean Access Manager can be configured to send traps by adding trap sinks. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

Step 1 Click the **Add New Trapsink** link in the upper-right-hand corner of the pane to bring up the Add New Trapsink form as shown in Figure 13-5.

Figure 13-5 Add New Trapsink



Step 2 Enter a **Trapsink IP**.

Step 3 Enter a **Trapsink Community** string.

Step 4 Enter an optional **Trapsink Description**.

Step 5 Click **Update** to update the SNMP Trapsink table.

Once trapsink configuration is complete, the Clean Access Manager will send DISMAN-EVENT style traps which refer to UCD table entries. The Clean Access Manager also sends traps if the root partition falls below a configured amount of space remaining (which defaults to 50%), and if the CPU load is above the configured amount for 1, 5 or 15 minutes.

Note The trapsink configured are used by all the Clean Access Servers connected to the Clean Access Manager.

A trap will contain the following contents:

Trap Contents	Description
Type: Enterprise-Specific(1)	
SNMP Trap OID (1.3.6.1.6.3.1.1.4.1.0)	Set to DISMAN-EVENT-MIB 2.0.1 (1.3.6.1.2.1.88.2.0.1)
The contents of a DISMAN mteObjectsEntry:	
mteHotTrigger (OID 1.3.6.1.2.1.88.2.1.1)	Generally: “process table” for processes “laTable” for load average alerts “dskTable” for disk capacity alerts “memory” for virtual memory alerts
mteHotTargetName (OID 1.3.6.1.2.1.88.2.1.2)	Always blank.
mteHotContextName (OID 1.3.6.1.2.1.88.2.1.3)	Always blank.
mteHotOID (OID 1.3.6.1.2.1.88.2.1.4)	Set to the OID of the UCD table that contains the data that triggered the event.
mteHotValue (OID 1.3.6.1.2.1.88.2.1.5)	Set to 0 if the trap is not an error Set to non-zero if an error condition is being reported (generally 1).
mteFailedReason (OID 1.3.6.1.2.1.88.2.1.6)	Set to a string describing the reason the alert was sent.

SNMP on Individual CAS

The configuration settings in Enable SNMP Polling/Alerts, page 13-13 are applied to all the Clean Access Servers connected to the Clean Acces Manager. If you want to change the configuration settings for one of the Clean Access Servers, you can specify the settings in the corresponding CAS, using any one of the following:

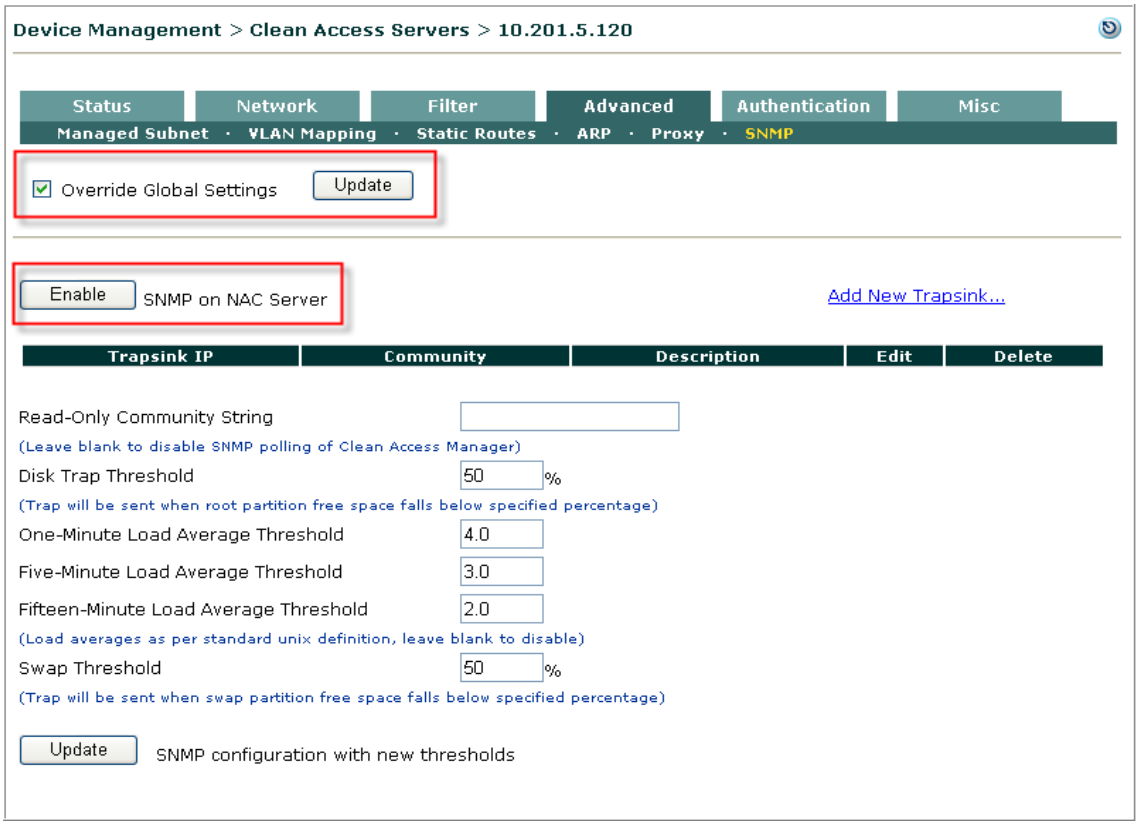
- In the CAS web console, navigate to **Administration > SNMP** and modify the configuration. Refer to the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for more details.

  [OR]

- In the CAM web console, go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > SNMP** and modify the configuration as described in the following procedure:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > SNMP** to bring up the SNMP configuration page (Figure 13-6).

Figure 13-6 Device Management > CCA Servers > Manage [CAS_IP] > Advanced > SNMP Page



Step 2 Check the **Override Global Settings** checkbox and click **Update** to override the configuration settings that have been already specified in the **Monitoring > SNMP** page.

Step 3 Click the **Enable** button preceding **SNMP on NAC Servers** to activate the SNMP polling and SNMP traps.

Step 4 Specify values for the following fields:

- **Read-Only Community String:**
  Specify a string to enable the Clean Access Server to respond to snmpget and snmpwalk requests with the correct community string. Leave this field blank to disable all Clean Access Server responses to SNMP polling of the Clean Access Server.
- **Disk Trap Threshold%:** (default is 50%)
  A trap will be sent when root partition free space falls below specified percentage.
- **One-Minute Load Average Threshold:** (default is 3.0)
  A trap will be sent when the one-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
- **Five-Minute Load Average Threshold:** (default is 2.0)
  A trap will be sent when the 5-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
- **Fifteen-Minute Load Average Threshold:** (default is 1.0)
  A trap will be sent when the 15-minute load average exceeds the threshold set here. Enter load averages as per standard unix definition.
- **Swap Threshold:** (default is 50%)
  A trap will be sent when swap partition free space falls below specified percentage.

Step 5 Click **Update** to update the SNMP configuration with new thresholds.

Add New Trapsink to CAS

The Clean Access Server can be configured to send traps by adding trap sinks. All traps sent are version 1 (v1) traps. A copy of each trap will be sent to each trapsink.

Step 1 Click the **Add New Trapsink** link in the upper-right-hand corner of the pane to bring up the Add New Trapsink form similar to Figure 13-5.

Step 2 Enter a **Trapsink IP**.

Step 3 Enter a **Trapsink Community** string.

Step 4 Enter an optional **Trapsink Description**.

Step 5 Click **Update** to update the SNMP Trapsink table.

Once trapsink configuration is complete, the Clean Access Server will send DISMAN-EVENT style traps which refer to UCD table entries. The Clean Access Server also sends traps if the root partition falls below a configured amount of space remaining (which defaults to 50%), and if the CPU load is above the configured amount for 1, 5 or 15 minutes.



Administering the CAM

This chapter discusses the Administration pages for the Clean Access Manager. Topics include:

- Overview, page 14-1
- Network, page 14-2
- Failover, page 14-4
- Set System Time, page 14-5
- Manage CAM SSL Certificates, page 14-7
- System Upgrade, page 14-24
- Licensing, page 14-25
- Policy Import/Export, page 14-28
- Support Logs, page 14-42
- Agent Logs, page 14-46
- Admin Users, page 14-47
- Manage System Passwords, page 14-56
- Backing Up the CAM Database, page 14-58
- API Support, page 14-65

For details on the User Pages module, see Chapter 5, "Configuring User Login Page and Guest Access."

For details on high availability configuration, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Overview

At installation time, the initial configuration script provides for many of the Clean Access Manager's internal administration settings, such as its interface addresses, DNS servers, and other network information. The Administration module (Figure 14-1) allows you to access and change these settings after installation has been performed.

Figure 14-1 Administration Module



The **CCA Manager** pages of the Administration module allows you to perform the following administration tasks:

- Change network settings for the Clean Access Manager. See Network, page 14-2.
- Set up Clean Access Manager High-Availability mode. See the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.
- Manage Clean Access Manager system time. See Set System Time, page 14-5.
- Manage Clean Access Manager SSL certificates. See Manage CAM SSL Certificates, page 14-7.
- Upload a software upgrade image onto the Clean Access Manager before performing console/SSH upgrade. See the "Upgrading to a New Software Release" section of the corresponding *Release Notes for Cisco NAC Appliance*.
- Manage Clean Access Manager license files. See Licensing, page 14-25.
- Create support logs for the CAM to send to customer support. See Support Logs, page 14-42.

The **User Pages** tabs of the Administration module allows you to perform these administration tasks:

- Add the default login page, and create or modify all web user login pages. See Chapter 5, "Configuring User Login Page and Guest Access."
- Upload resource files to the Clean Access Manager. See Upload a Resource File, page 5-13.

The **Admin Users** pages of the Administration module (see Admin Users, page 14-47) allows you to perform these administration tasks:

- Add and manage new administrator groups and admin users/passwords
- Configure and manage Administrator privileges as new features are added

The **Backup** page of the Administration module allows you to make manual snapshots of your Clean Access Manager in order to backup your CAM's configuration. See Backing Up the CAM Database, page 14-58.

In addition, the CAM provides an API interface described in API Support, page 14-65.

Network

You can view or change the Clean Access Manager's network settings from **Administration > CCA Manager > Network** page.

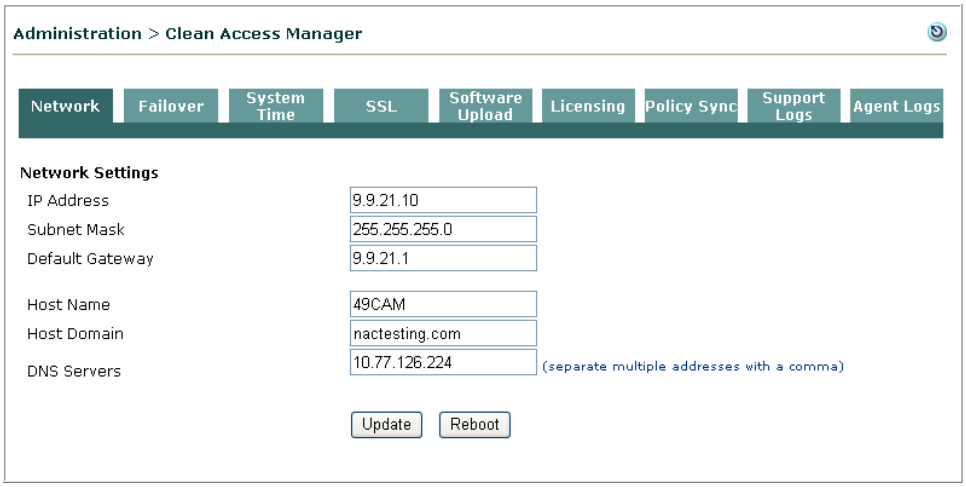
Changes to the network settings generally require a reboot of the Clean Access Manager machine to take effect. Therefore, if making changes to a production machine, make sure to perform the changes when rebooting the machine will have minimal impact on the users.

Note The **`service perfigo config`** configuration utility script also lets you modify CAM network settings. Because the configuration utility is used from the command line, it is particularly useful if the admin console web server is not responsive due to incorrect network or VLAN settings. For further details, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

To modify CAM network settings:

Step 1 Go to **Administration > CCA Manager > Network**.

Figure 14-2 CAM Network



Step 2 In the **Network** page, modify the settings as desired from the following fields/controls:

- **IP Address**—The eth0 IP address of the CAM machine.
- **Subnet Mask**—The subnet mask for the IP address.
- **Default Gateway**—The default IP gateway for the CAM.
- **Host Name**—The host name for the CAM. The name is required in high availability mode.
- **Host Domain**—An optional field for your domain name suffix. To resolve a host name to an IP address, the DNS requires the fully qualified host name. Within a network environment, users often type host names in a browser without a domain name suffix, for example:

  `http://siteserver`

  The host domain value is used to complete the address. For example, with a suffix value of cisco.com, the request URL would be:

  `http://siteserver.cisco.com`

- **DNS Servers**—The IP address of the DNS (Domain Name Service) server in your environment. Separate multiple addresses with commas. If you specify more than one DNS server, the Clean Access Manager tries to contact them one by one, and stops when it receives a response.

Note If the setup is in HA mode, then go to **Administration > CCA Manager > Failover**. Enter appropriate values in the **Failover** page and click **Update**.

Step 3 Click **Reboot** to restart the Clean Access Manager with the new settings.

Failover

You can view or change the Clean Access Manager's failover settings from **Administration > CCA Manager > Failover** page.

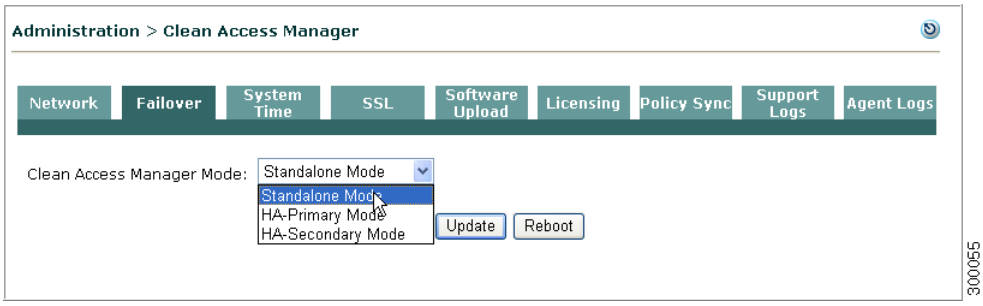
Changes to the network settings generally require a reboot of the Clean Access Manager machine to take effect. Therefore, if making changes to a production machine, make sure to perform the changes when rebooting the machine will have minimal impact on the users.

Note The `service perfigo config` configuration utility script also lets you modify CAM network settings. Because the configuration utility is used from the command line, it is particularly useful if the admin console web server is not responsive due to incorrect network or VLAN settings. For further details, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

To modify CAM failover settings:

Step 1 Go **Administration > CCA Manager > Failover**.

Figure 14-3 CAM Failover



Step 2 In the **Network** page, modify the CAM's operating mode using the **Clean Access Manager Mode** menu:

- **Standalone Mode**—If the Clean Access Manager is operating alone.
- **HA-Primary Mode**—For the primary Clean Access Manager in a failover configuration.
- **HA-Standby Mode**—For the secondary Clean Access Manager.

  If you choose one of the HA (high availability) options, additional fields appear. For information on the fields and setting up high availability, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Step 3 Click the **Update** button.

Set System Time

For logging purposes and other time-sensitive tasks (such as SSL certificate generation), the time on the Clean Access Manager and Clean Access Servers needs to be correctly synchronized. The **System Time** tab lets you set the time on the Clean Access Manager and modify the time zone setting for the Clean Access Manager operating system.

After CAM and CAS installation, you should synchronize the time on the CAM and CAS before regenerating a temporary certificate on which a Certificate Signing Request (CSR) will be based. The easiest way to ensure this is to automatically synchronize time with the time server (**Sync Current Time** button).

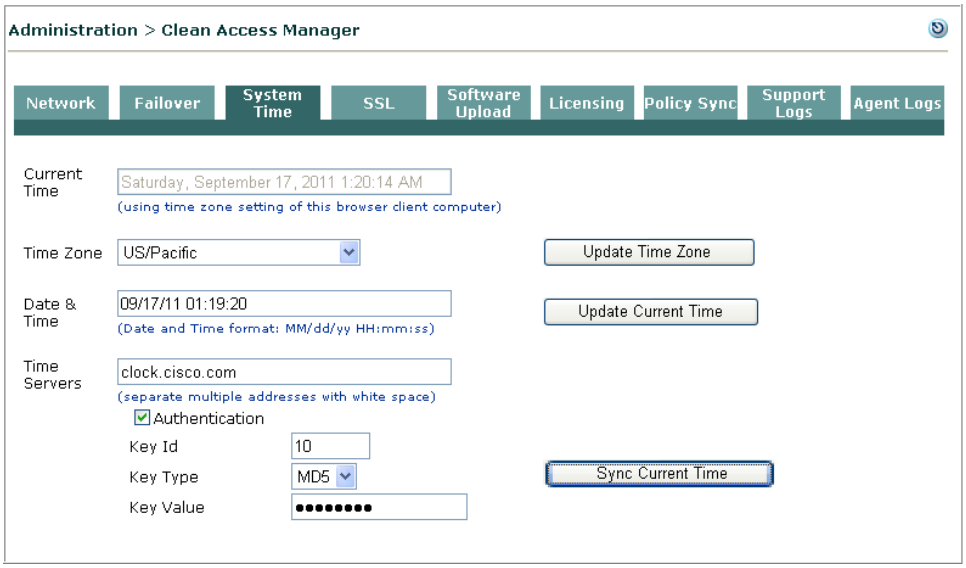
Note The time set on the CAS must fall within the creation date/expiry date range set on the CAM's SSL certificate. The time set on the user machine must fall within the creation date/expiry date range set on the CAS's SSL certificate.

The time can be modified on the CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Time**. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

To view the current time:

1. Go to **Administration > CCA Manager > System Time**.
2. The system time for the Clean Access Manager appears in the **Current Time** field.

Figure 14-4 System Time



There are two ways to adjust the system time: manually, by typing in the new time, or automatically, by synchronizing from an external time server.

To manually modify the system time:

1. In the **System Time** form, either:
2. Type the time in the **Date & Time** field and click **Update Current Time**. The time should be in the form: *mm/dd/yy hh:ss* PM/AM
3. Or, click the **Sync Current Time** button to have the time updated by the time servers listed in the **Time Servers** field.

To automatically synchronize to the time server:

The default time server is the server managed by the National Institute of Standards and Technology (NIST), at **time.nist.gov**. To specify another time server:

1. In the **System Time** form type the URL of the server in the **Time Servers** field. The server should provide the time in NIST-standard format. Use a space to separate multiple servers.
2. If you want to authenticate the server to get the time, check the **Authentication** checkbox to enable NTP authentication. Once this option is enabled, you will be able to enter the following:
   - **Key Id**—Specify a key number.
   - **Key Type**—Currently, only MD5 is supported. The key type **MD5** specifies that message authentication support is provided by using the Message Digest 5 hashing algorithm.
   - **Key Value**—For MD5 authentication, this is a password consisting of a string of one to eight characters. If the string is longer than eight characters, only the first eight will be used.

Note The NTP Authentication is not available for FIPS-compliant CAMs/CASs.

3. Click **Sync Current Time**.

If more than one time server is listed, the CAM tries to contact the first server in the list when synchronizing. If available, the time is updated from that server. If it is not available, the CAM tries the next one, and so on, until a server is reached.

Note If the NTP Authentication has been enabled, the same Key Id, Key Type, and Key value are used for all the servers.

To poll the time server periodically, edit the **ntp.conf** file and then start ntpd as follows:

```
[root@cam1 init.d]# ./ntpd
Usage: ./ntpd {start|stop|restart|condrestart|status}
[root@cam1 init.d]# ./ntpd start
Starting ntpd: [  OK  ]
```

To change the time zone of the server system time:

1. In the **Current Time** tab of the **Administration > CCA Manager** page, choose the new time zone from the **Time Zone** drop-down list.
2. Click **Update Time Zone**.

Manage CAM SSL Certificates

This section describes the following:

- SSL Certificate Overview, page 14-7
- Web Console Pages for SSL Certificate Management, page 14-8
- Typical SSL Certificate Setup on the CAM, page 14-9
- Generate Temporary Certificate, page 14-11
- Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12
- Manage Signed Certificate/Private Key, page 14-14
- Manage Trusted Certificate Authorities, page 14-16
- View Current Private Key/Certificate and Certificate Authority Information, page 14-19
- Troubleshooting Certificate Issues, page 14-21

SSL Certificate Overview

The elements of Cisco NAC Appliance communicate securely over Secure Socket Layer (SSL) connections. Cisco NAC Appliance uses SSL connections for a number of purposes, including the following:

- Secure communications between the CAM and the CAS

Caution CAM-CAS communication and HA-CAM and/or HA-CAS peer communication can break down and adversely affect network functionality when SSL certificates expire. For more information, see HA Active-Active Situation Due to Expired SSL Certificates, page 14-21.

- Policy Import/Export operations between Policy Sync Master and Policy Sync Receiver CAMs
- CAM-to-LDAP authentication server communications where SSL has been enabled for the **LDAP** authentication provider using the **Security Type** option on the **User Management > Auth Servers > New | Edit** page
- Between the CAS and end-users connecting to the CAS
- Between the CAM/CAS and the browsers accessing the CAM/CAS web admin consoles

During installation, the configuration utility script for both the CAM and CAS requires you to generate a temporary SSL certificate for the appliance being installed (CAM or CAS). For the Clean Access Manager and Clean Access Servers operating strictly in a lab environment, it is not necessary to use a CA-signed certificate and you can continue to use a temporary certificate, if desired. For security reasons in a production deployment, however, you must replace the temporary certificate for the CAM and CAS with a third-party CA-signed SSL certificate.

At installation, a corresponding Private Key is also generated with the temporary certificate. Cisco NAC Appliance Release 4.7(0) uses two types of keys to support FIPS compliance: Private Keys and Shared Master Keys. Both of these key types are managed and stored using the FIPS card installed in the CAM/CAS. During installation, keys are created using the CAM/CAS setup utilities, the keys are then *moved* to the FIPS card for security, and key-generation files and/or directories are then removed from the CAM/CAS.

In Cisco NAC Appliance Release 4.8 and later, you can no longer export private keys and you cannot generate CSRs using a FIPS 140-2 compliant CAM/CAS. To adhere to FIPS compliance guidelines, you can only import certificates from trusted third-party resources.

For details on managing SSL certificates for the CAS, see the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Note Cisco NAC Appliance supports 1024-, 2048-, and 4096-bit RSA key lengths for SSL certificates.

Note Cisco NAC Appliance supports Extended Validation (EV) SSL certificates.

Note Cisco NAC Appliance does not support wildcard SSL certificates.

The following sections describe how to manage SSL certificates for the CAM:

- Generate Temporary Certificate, page 14-11
- Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12
- Manage Signed Certificate/Private Key, page 14-14
- Manage Trusted Certificate Authorities, page 14-16
- View Current Private Key/Certificate and Certificate Authority Information, page 14-19
- Troubleshooting Certificate Issues, page 14-21

Note You cannot use a CA-signed certificate that you bought for the Clean Access Manager on the Clean Access Server. You must buy a separate certificate for each Clean Access Server.

Web Console Pages for SSL Certificate Management

The actual CAM SSL certificate files are kept on the CAM machine, and the CAS SSL certificate files are kept on the CAS machine. After installation, the CAM certificates are managed from the following web console pages (respectively):

Clean Access Manager Certificates:

- **Administration > CCA Manager > SSL > X509 Certificate**—Use this configuration window to import and export temporary or CA-signed certificates, import Private Keys (FIPS and non-FIPS appliances), export Private Keys (non-FIPS appliances only), and generate new temporary certificates
- **Administration > CCA Manager > SSL > Trusted Certificate Authorities**—Use this configuration window to view, add, and remove Certificate Authorities on the CAM
- **Administration > CCA Manager > SSL > X509 Certification Request** (non-FIPS appliances only)—Use this configuration window to generate a new Certificate Signing Request (CSR) for the CAM

The CAM web admin console lets you perform the following SSL certificate-related operations:

- Generate a PEM-encoded PKCS #10 CSRs (non-FIPS appliances only).

- Import (FIPS and non-FIPS) and export (non-FIPS only) Private Keys. For non-FIPS appliances, you can use this feature to save a backup copy of the Private Key on which the CSR is based. When a CA-signed certificate is returned from the Certificate Authority and imported into the CAM (FIPS and non-FIPS), this Private Key must be used with it or the CAM cannot communicate with any associated machines via SSL.
- View, remove, and import/export Trusted CAs in the CAM local trust store.
- Generate a temporary certificates (and corresponding Private Keys). Temporary certificates are designed for lab environments only. When you deploy your CAM and CAS in a production environment, Cisco strongly recommends using a trusted certificate from a third-party Certificate Authority to help ensure network security.

Typical SSL Certificate Setup on the CAM

Some typical steps for managing CAM certificates are as follows.

Phase 1: Prepare Your CAM and CAS for the Certificate Signing Request (CSR)

Step 1 Synchronize time.

After CAM and CAS installation, make sure the time on the CAM and CAS is synchronized before regenerating the temporary certificate on which the Certificate Signing Request will be based. See the next section, Set System Time, page 14-5, for details.

Step 2 Check DNS settings for the CAM.

If planning to use the DNS name instead of the IP address of your servers for CA-signed certificates, you will need to verify the CAM settings and regenerate a temporary certificate. See Regenerating Certificates for DNS Name Instead of IP, page 14-23 for details.

Step 3 Generate Temporary Certificate, page 14-11.

A temporary certificate and Private Key are automatically generated during CAM installation. If changing time or DNS settings on the CAM, regenerate the temporary certificate and Private Key.

Step 4 Ensure you export the certificate from your CAM, save it on a machine accessible from your CAS, and import the exported certificate on the CAS, and repeat the process in reverse to ensure the CAS certificate also resides on the CAM.

Phase 2: Prepare your CAM and CAS For CA-Signed Certs (Production Deployment)

Warning **If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.5 and later. You must correct your certificate chain to successfully upgrade to release 4.5 and later. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

Step 5 Export (Backup) the certificate to a local machine for safekeeping.

If you are altering your Cisco NAC Appliance SSL configuration, it is always a good idea to back up the certificate to a local hard drive for safekeeping. See Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12.

Step 6 (Non-FIPS appliances only) Export the Private Key to a local machine for safekeeping

If you are altering your Cisco NAC Appliance SSL configuration, it is always a good idea to back up the Private Key corresponding to the current certificate to a local hard drive for safekeeping. See Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12.

Step 7 (Non-FIPS appliances only) Export (save) the Certificate Signing Request (CSR) to a local machine. See Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12.

Step 8 Send the CSR file to a Certification Authority (CA) authorized to issue trusted certificates.

Step 9 After the CA signs and returns the certificate, import the CA-signed certificate to your server.

When the CA-signed certificate is received from the CA, upload it as PEM-encoded file to the CAM temporary store. See Manage Signed Certificate/Private Key, page 14-14.

Note The CAM and CAS require encrypted communication. Therefore, the CAM must contain the Trusted Certificate Authorities from which the certificates on all of its managed CASs originate, and all CASs must contain the same Trusted Certificate Authority from which the CAM certificate originates before deploying Cisco NAC Appliance in a production environment.

Step 10 If necessary, upload any required intermediate CA certificate(s) as a single PEM-encoded file to the CAM temporary store.

Step 11 Test access to the Clean Access Manager.

Note Make sure the CA-signed certificate you are importing is the one with which you generated the CSR and that you have NOT subsequently generated another temporary certificate. Generating a new temporary certificate will create a new private-public key combination. In addition, always export and save the Private Key to a secure location when you are generating a CSR for signing (for safekeeping and to have the Private Key handy).

For additional details, see also Troubleshooting Certificate Issues, page 14-21.

Phase 3: Adding a New CAM or CAS to an Existing Production Deployment

In production deployments and for FIPS 140-2 compliant appliances, CA-signed certificates are used exclusively. Use the following steps when introducing new appliances (CAM or CAS) to a production deployment. The new appliance should not be added to the deployment until you have requested and are able to import a new third-party CA-signed certificate.

Step 1 Install and initially configure the new appliance as described in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Step 2 Follow the steps in Phase 1: Prepare Your CAM and CAS for the Certificate Signing Request (CSR), page 14-9

Step 3 (Non-FIPS appliances only) Generate a CSR for the new appliance, as described in Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12.

Step 4 Obtain and install the CA-signed certificate as described in Import Signed Certificate/Private Key, page 14-14.

Step 5 Add the appliance to your existing production environment.

Generate Temporary Certificate

The following procedure describes how to generate a new temporary certificate for the CAM. Any time you change basic configuration settings on the CAM (date, time, associated DNS server, etc.) you should generate a new temporary certificate.

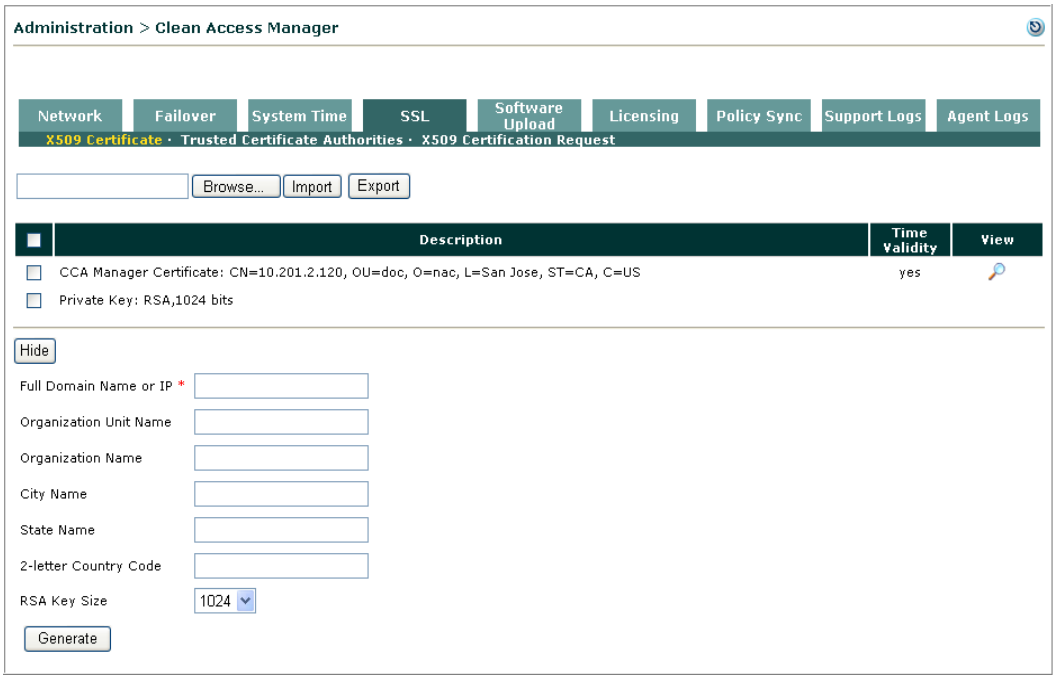
Caution If you are using FIPS 140-2 compliant appliances, be sure you have your current trusted-CA certificate and Private Key stored on an external machine so you can restore them following this procedure.

If you are using a CA-signed certificate on a non-FIPS appliance, Cisco recommends backing up the Private Key for the current certificate prior to generating any new certificate, as generating a new certificate also generates a new Private Key. See Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12 for more information.

Step 1 Go to **Administration > CCA Manager > SSL > X509 Certificate**.

Step 2 Click **Generate Temporary Certificate** to expose the fields required to construct a temporary certificate (Figure 14-5).

Figure 14-5 Generate Temporary Certificate



Step 3 Type appropriate values for the following fields:

- **Full Domain Name or IP**—The fully qualified domain name or IP address of the Clean Access Manager for which the certificate is to apply. For example: `camanager.<your_domain_name>`
- **Organization Unit Name**—The name of the unit within the organization, if applicable.
- **Organization Name**—The legal name of the organization.
- **City Name**—The city in which the organization is legally located.
- **State Name**—The full name of the state in which the organization is legally located.
- **2-letter Country Code**—The two-character, ISO-format country code, such as GB for Great Britain or US for the United States.

Step 4 Specify whether you want the new temporary certificate to use a 1024-, 2048-, or 4096-bit **RSA Key Size**.

Step 5 When finished, click **Generate**. This generates a new temporary certificate and new Private Key.

Step 6 For FIPS 140-2 compliant appliances, be sure to be sure to restore your current trusted-CA certificate and Private Key from an external machine.

Note The **CCA Manager Certificate** entry at the top of the certificate display table specifies the full distinguished name of the current CAM SSL certificate. You are required to enter the full distinguished name of the CAM in the CAS web console if you are setting up Authorization between your CAM and CASs. For more information, see Configure Clean Access Manager-to-Clean Access Server Authorization, page 2-5.

Generate and Export a Certification Request (Non-FIPS CAM Only)

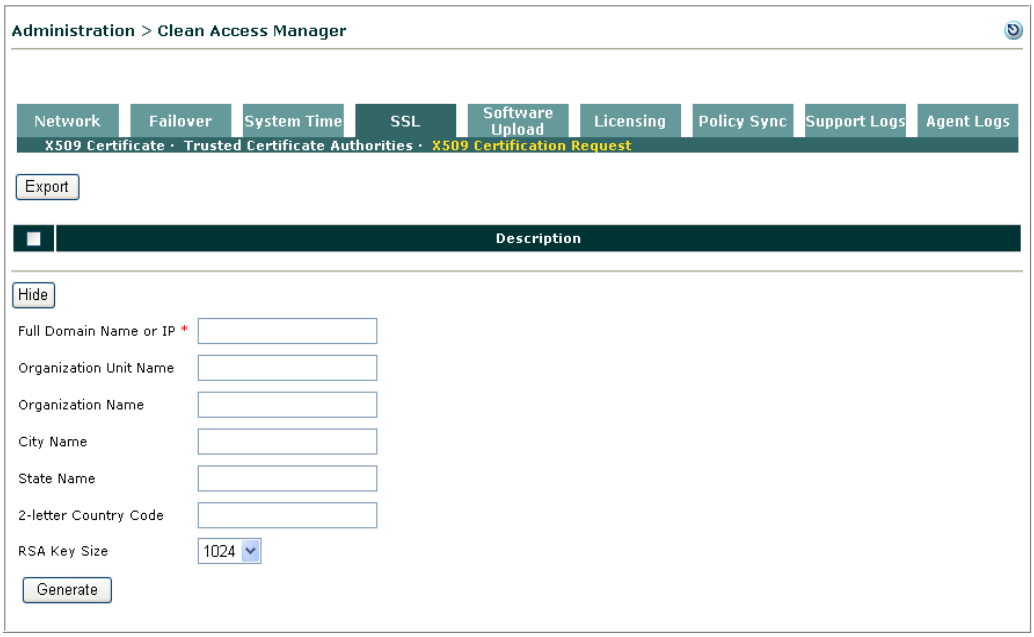
Note The **Administration > CCA Manager > SSL > X509 Certification Request** subtab does not appear in the CAM web console on a FIPS 140-2 compliant appliance.

Generating a CSR creates a PEM-encoded PKCS#10-formatted Certificate Signing Request (CSR) suitable for submission to a certificate authority. Before you send the CSR, make sure to export the existing certificate and Private Key to a local machine to back it up for safekeeping.

To export he CSR/Private Key and create a certificate request from the CAM web console:

Step 1 Go to **Administration > CCA Manager > SSL > X509 Certification Request** (Figure 14-6).

Figure 14-6 Export CSR/Private Key



Step 2 Click **Generate Certification Request** to expose the fields required to construct a certificate request.

Step 3 Type appropriate values for the following fields:

- **Full Domain Name or IP**—The fully qualified domain name or IP address of the Clean Access Manager for which the certificate is to apply. For example: `camanager.<your_domain_name>`
- **Organization Unit Name**—The name of the unit within the organization, if applicable.
- **Organization Name**—The legal name of the organization.
- **City Name**—The city in which the organization is legally located.
- **State Name**—The full name of the state in which the organization is legally located.
- **2-letter Country Code**—The two-character, ISO-format country code, such as GB for Great Britain or US for the United States.

Step 4 Specify whether you want the new temporary certificate to use a 1024-, 2048-, or 4096-bit **RSA Key Size**.

Step 5 Click **Generate** to generate a certificate request. Make sure these are the ones for which you want to submit the CSR to the certificate authority.

Step 6 Before you submit the new CSR to the Certificate Authority, save the new certification request and Private Key used to generate the request to your local machine by enabling the checkboxes for the **Certification Request** and/or **Private Key** and clicking **Export**. You are prompted to save or open the file (see Default File Names for Exported Files, page 14-14). Save it to a secure location. Use the CSR file to request a certificate from a certificate authority. When you order a certificate, you may be asked to copy and paste the contents of the CSR file into a CSR field of the order form.

Alternatively, you can immediately **Open** the CSR in Wordpad or a similar text editor if you are ready to fill out the certificate request form, but Cisco strongly recommends you also save a local copy of the CSR and Private Key to ensure you have them should the request process suffer some sort of mishap or your CAM basic configuration change between submitting the CSR and receiving your CA-signed certificate.

When you receive the CA-signed certificate back from the certification authority, you can import it into the Clean Access Manager as described in Manage Signed Certificate/Private Key, page 14-14. After the CA-signed cert is imported, the "currently installed certificate" is the CA-signed certificate. You can always optionally **Export** the currently installed certificate if you need to access a backup of this certificate later.

Default File Names for Exported Files

The default file names for SSL Certificate files that can be exported from the CAM are as follows. When you actually save the file to your local machine, you can specify a different name for the file. For example, to keep from overwriting your **chain.pem** file containing your certificate chain information, you can specify your Private Key filename to be a more appropriate name like **priv_key.pem** or something similar.

Default File Name [1]	Description
cert_request.pem	CAM Certificate Signing Request (CSR)
chain.pem[2]	CAM Currently Installed Certificate and Currently Installed Private Key

1. For release 3.6.0.1 and below the filename extension is .csr instead of .pem.
2. For release 3.6(1) only, the filename is smartmgr_crt.pem.

Manage Signed Certificate/Private Key

Import Signed Certificate/Private Key

You can import CA-signed PEM-encoded X.509 Certificates and Private Keys using the CAM web console on both FIPS 140-2 compliant and non-FIPS appliances. (Typically, you only need to re-import the Private Key if the current Private Key does not match the one used to create the original CSR on which the CA-Signed certificate is based.) There are two methods administrators can use to import CA-signed certificates, Private Keys, and associated Certificate Authority information into Cisco NAC Appliance:

1. Import the Certificate Authorities and the End Entity Certificates/Private Keys separately:
   a. Import the Certificate Authorities into the trust store using the procedures in Manage Trusted Certificate Authorities, page 14-16
   b. Import the CAM's end entity certificate and/or Private Key using the instructions below
2. Construct a PEM-encoded X.509 certificate chain (including the Private Key, End Entity, Root CA, and Intermediate CA certificates) and import the entire chain at once using the instructions below

If you have received a CA-signed PEM-encoded X.509 certificate for the Clean Access Manager, you can also import it into the Clean Access Manager as described here.

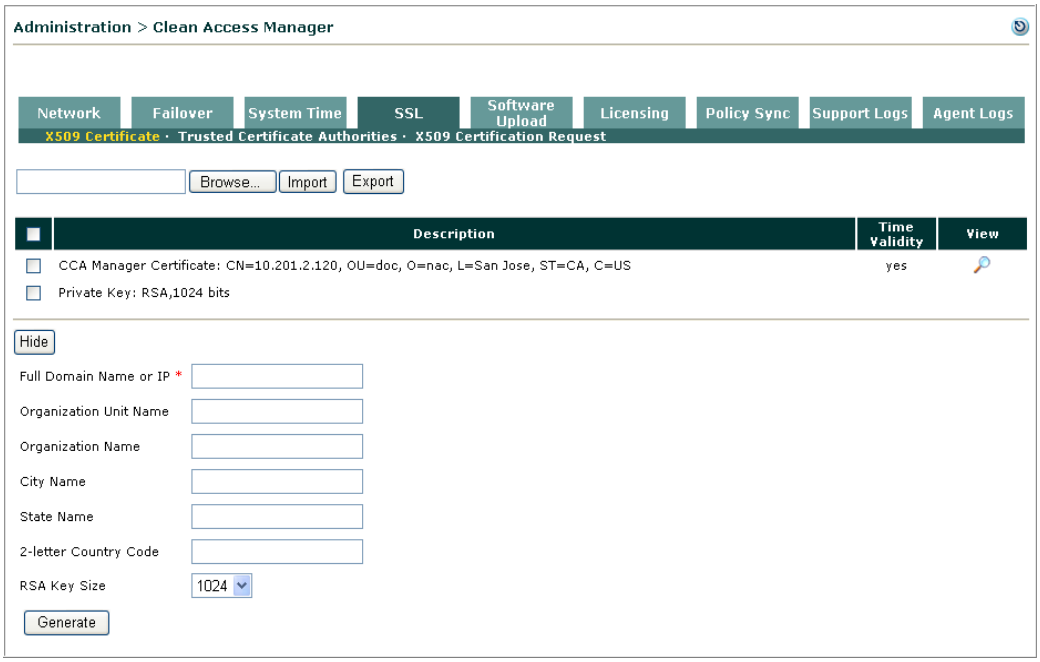
Before starting, make sure that the root and CA-signed certificate files are in an accessible file directory location and that you have obtained third-party certificates for both your CAM and CASs. If using a Certificate Authority for which intermediate CA certificates are necessary, make sure these files are also present and accessible if not already present on the CAM.

Note Any certificate that is not provided by a public CA or that is not the self-signed certificate is considered a non-standard certificate by the CAM/CAS. When importing certificates to the CAM, make sure to obtain CA-signed certificates for authentication servers.

To import a certificate and/or Private Key for the CAM:

Step 1 Go to **Administration > CCA Manager > SSL > X509 Certificate** (Figure 14-7).

Figure 14-7 Import Certificate (CAM)



Step 2 Click **Browse** and locate the certificate file and/or Private Key on your local machine.

Note Make sure there are no spaces in the filename when importing files (you can use underscores).

Step 3 Click **Import**.

Note Neither the CAM nor CAS will install an unverifiable certificate chain. You must have delimiters (Begin/End Certificate) for multiple certificates in one file, but you do not need to upload certificate files in any particular sequence because they are verified in the temporary store first before being installed.

If you already have other members of the certificate chain in the CAM trust store, you do not need to re-import them. The CAM can build the certificate chain from a combination of newly-imported and existing parts.

If you try to upload a root/intermediate CA certificate for the CAM that is already in the list, you may see an error message reading "This intermediate CA is not necessary." In this case, you must delete the uploaded Root/Intermediate CA in order to remove any duplicate files.

Export Certificate and/or Private Key

Note You cannot export the Private Key for a FIPS 140-2 compliant CAM. You can only export certificates.

To backup your certificate and/or Private Key in case of system failure or other loss, you can export your certificate and/or Private Key information and save a copy on your local machine. This practice also helps you manage certificate/Private Key information for a CAM HA-Pair. By simply exporting the certificate information from the HA-Primary CAM and importing it on the HA-Secondary CAM, you are able to push an exact duplicate of the certificate info required for CAM/CAS communication to the standby CAM.

Step 1 Go to **Administration > CCA Manager > SSL > X509 Certificate** (Figure 14-7).

Step 2 To export existing certificate/Private Key information:

a. Select one or more certificates and/or the Private Key displayed in the certificates list by clicking on their respective left hand checkboxes.

b. Click **Export** and specify a location on your local machine where you want to save the resulting file.

Manage Trusted Certificate Authorities

You can locate, remove, and import/export Trusted CAs for the CAM database using the **Administration > CCA Manager > SSL > Trusted Certificate Authorities** CAM web console page. To keep your collection of trusted certificate authorities easily manageable, Cisco recommends keeping only trusted certificate authority information critical to Cisco NAC Appliance operations in the CAM trust store.

You can also use this function to import Root and Intermediate Certificate Authorities.

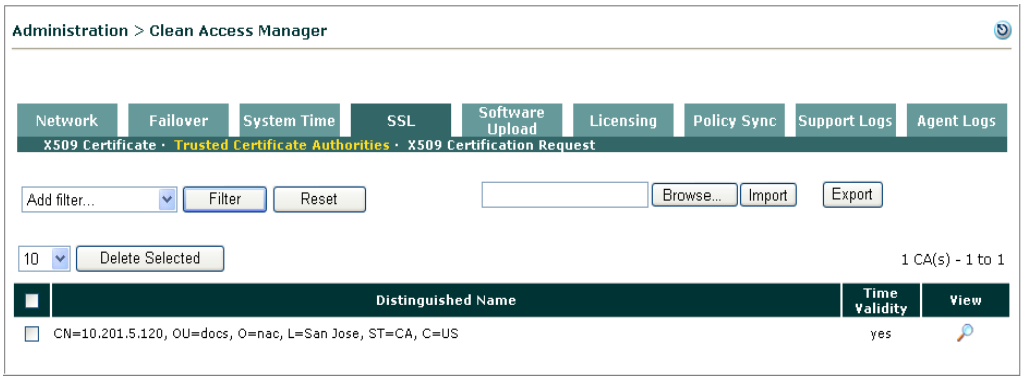
Note You must upload the PEM-encoded CA-signed certificate on both the CAM and CASs in your Cisco NAC Appliance network.

If there are multiple Intermediate CA files, you can also copy and paste them into a single Intermediate CA PEM-encoded file for upload to the CAM using the procedure in Manage Signed Certificate/Private Key, page 14-14.

To view and/or remove Trusted CAs from the CAM:

Step 1 Go to **Administration > CCA Manager > SSL > Trusted Certificate Authorities** (Figure 14-8).

Figure 14-8 CAM Trusted Certificate Authorities



Viewing Trusted CAs

Step 2 If you want to refine the list of Trusted CAs displayed in the CAM web console:

a. Choose an option from the **Filter** dropdown menu:

- **Distinguished Name**—Use this option to refine the list of Trusted CAs according to whether the Trusted CA name contains or does not contain a specific text string.
- **Time**—Use this option to refine the display according to which Trusted CAs are currently valid or invalid.

  You can also combine these two options to refine the Trusted CAs display.

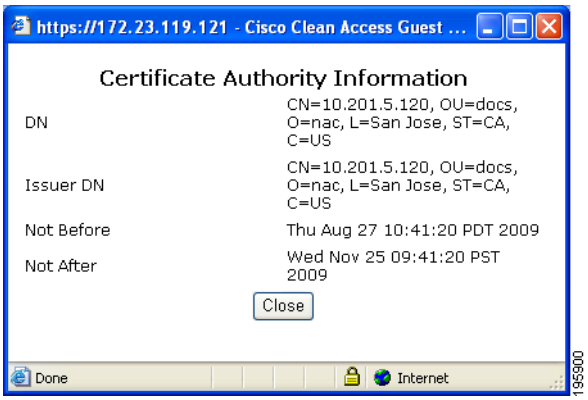
b. Click the **Filter** button after selecting and defining parameters for the search options to display a refined list of all Trusted CAs that match the criteria.

You can click **Reset** to negate any of the optional search criteria from the filter dropdown menu and return the Trusted CA display to default settings.

c. You can also increase or decrease the number of viewable items in the Trusted CAs list by choosing one of the options in the dropdown menu at the top-left of the list. The options are 10, 25, or 100 items.

d. If you want to view details about an existing Trusted CA, click the **View** icon (far-right magnifying glass icon) to see information on the specific certificate authority, as shown in Figure 14-9.

Figure 14-9 Certificate Authority Information



Removing Trusted CAs

Step 3 Select one or more Trusted CAs to remove by clicking on the checkbox for the respective Trusted CA in the list. (Clicking on the empty checkbox at the top of the Trusted CAs display automatically selects or unselects *all* 10, 25, or 100 Trusted CAs in the viewable list.)

Step 4 Click **Delete Selected**. All viewable selected items will be deleted. For example, if you selected 25 items from the viewable item dropdown, and clicked the empty checkbox at the top of the Trusted CAs window, the 25 viewable items will be deleted.

Once the CAM removes the selected Trusted CAs from the database, the CAM automatically restarts services to complete the update.

Import/Export Trusted Certificate Authorities

You can use the Trusted Certificate Authorities web console page to import and export Certificate Authorities for the CAM.

Note For standard certificate import and export guidelines, refer to Generate and Export a Certification Request (Non-FIPS CAM Only), page 14-12 and Manage Signed Certificate/Private Key, page 14-14.

Step 1 Go to **Administration > CCA Manager > SSL > Trusted Certificate Authorities** (Figure 14-8).

Step 2 To import a Trusted Certificate Authority:

a. Ensure you have the appropriate certificate file accessible to the CAM in the network and click **Browse**.

b. Locate and select the certificate file on your directory system and click **Open**.

c. Click **Import** to upload the Trusted Certificate Authority information to your CAM.

Step 3 To export existing Trusted Certificate Authority information:

a. Select one or more Trusted CAs displayed in the Trusted Certificate Authorities list by clicking on their respective left hand checkboxes.

b. Click **Export** and specify a location on your local machine where you want to save the resulting "caCerts" file.

View Current Private Key/Certificate and Certificate Authority Information

You can verify the following files by viewing them under **Administration > CCA Manager > SSL > X509 Certificate** (Figure 14-5):

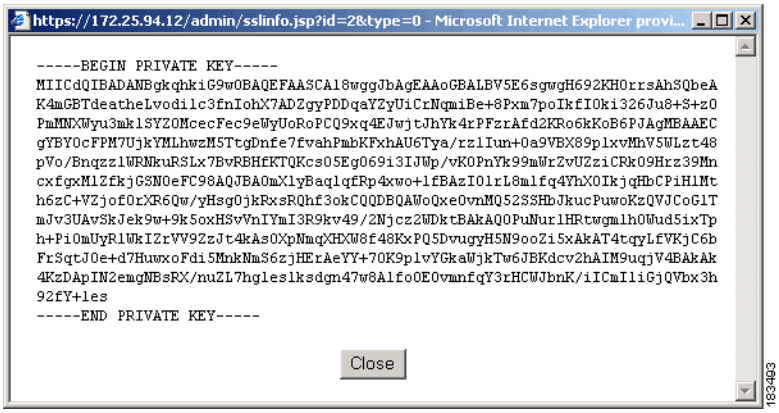
- Currently Installed Private Key
- Currently Installed End Entity, Root, and Intermediate CA Certificate
- Certificate Authority Information

Note You must be currently logged into your web console session to view any Private Key and/or certificate files.

View Currently Installed Private Key

You can view the CAM Private Key by exporting and opening the exported Private Key file in Wordpad or a similar text editor tool to bring up a dialog like the one in Figure 14-10 (BEGIN PRIVATE KEY/END PRIVATE KEY).

Figure 14-10 View Currently Installed Private Key

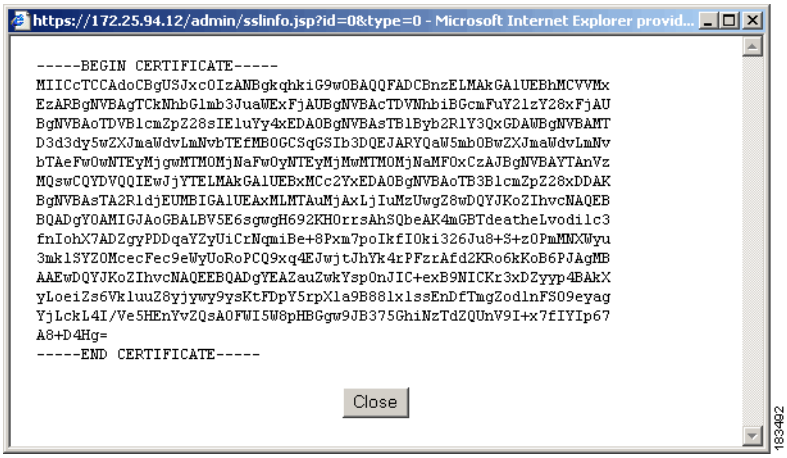


You can also use this method to view uploaded Private Keys before importing them into your CAM.

View Currently Certificate or Certificate Chain

You can view CAM Private Key and End Entity, Root CA, and Intermediate CA certificates by exporting and opening the saved file in Wordpad or a similar text editor tool to bring up a dialog like the one in Figure 14-11 (BEGIN CERTIFICATE/END CERTIFICATE).

Figure 14-11 View Currently Installed Certificate

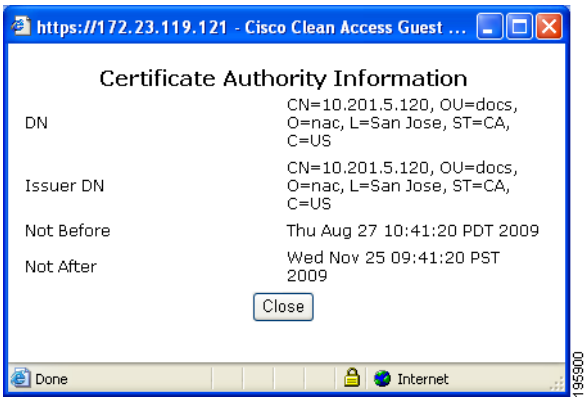


You can also use this method to view uploaded certificates before importing them into your CAM.

View Certificate Authority Information

You can view Certificate Authority information for CAM End Entity, Root, and Intermediate CA Certificates by clicking on the respective **View** icon (magnifying glass) in the right hand column to bring up a dialog like the one in Figure 14-12.

Figure 14-12 View Certificate Authority Information



Troubleshooting Certificate Issues

Issues can arise during Cisco NAC Appliance certificate management, particularly if there are mismatched SSL certificates somewhere along the certificate chain. Common problems on SSL certificates can be time-oriented (if the clocks are not synchronized on the CAM and CAS, authentication fails), IP-oriented (certificates are created for the wrong interface) or information-oriented (wrong or mistyped certificate information is imported). This section describes the following:

- HA Active-Active Situation Due to Expired SSL Certificates
- No Web Login Redirect/CAS Cannot Establish Secure Connection to CAM
- Private Key in Clean Access Server Does Not Match the CA-Signed Certificate
- Regenerating Certificates for DNS Name Instead of IP
- Disabling Administrator Prompt for Certificate on IE 8 and 9
- Certificate-Related Files

Warning **If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.5 and later. You must correct your certificate chain to successfully upgrade to release 4.5 and later. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

HA Active-Active Situation Due to Expired SSL Certificates

HA communication for both HA-CAMs and HA-CASs is handled over IPSec tunnels to secure all communications between the two HA pair appliances. This IPSec tunnel is negotiated based on the SSL certificates uploaded to the HA pairs for both CAM and CAS. In case the SSL certificates are not trusted by the two HA peers, have expired, or are no longer valid, the HA heartbeat communication between the two HA pairs breaks down, leading both HA pair appliances to assume the Active HA-Primary) role.

For CASs deployed in VGW mode, this can potentially create a Layer 2 loop that could bring down the network. HA-CAMs with expired or invalid SSL certificates could lead to an Active-Active situation where the database is not synced between the two HA-CAM appliances. Eventually, this situation leads to the CAMs losing all recent configuration changes and/or all recent user login information following an HA-CAM failover event.

As HA communication over IPSec tunnels requires valid SSL certificates on both the CAM and CAS, the CAM-CAS communication also breaks down if the SSL certificate expires on either the CAM or CAS. This situation leads to end user authentications failures and the CAS reverting to fallback mode per CAS configuration.

Administrators can minimize HA appliance Active-Active situations due to expired SSL certificates by using SSL certificates with longer validity periods and/or using serial port connection (if available and not used to control another CAM or CAS) for HA heartbeat. However, when you configure HA-CAMs to perform heartbeat functions over the serial link and the primary eth1 interface fails because of SSL certificate expiration, the CAM returns a database error indicating that it cannot sync with its HA peer and the administrator receives a “WARNING! Closed connections to peer [standby IP] database! Please restart peer node to bring databases in sync!!” error message in the CAM web console:

Note Starting with Cisco NAC Appliance Release 4.8, the CAM or CAS generates event log messages to indicate the certificate expiry in addition to the message displayed in the CAM/CAS web console.

No Web Login Redirect/CAS Cannot Establish Secure Connection to CAM

The following client connection errors can occur if the CAS does not trust the certificate of the CAM, or vice-versa:

- No redirect after web login— users continue to see the login page after entering user credentials
- Agent users attempting login get the following error: "Clean Access Server could not establish a secure connection to the Clean Access Manager at <IPaddress or domain>."

These errors typically indicate one of the following certificate-related issues:

- The time difference between the CAM and CAS is greater than 5 minutes
- Invalid IP address
- Invalid domain name
- CAM is unreachable

To identify common issues:

1. Check the CAM's certificate and verify it has not been generated with the IP address of the CAS.
2. Check the time set on the CAM and CAS. The time set on the CAM and the CAS must be 5 minutes apart or less.

To resolve these issues:

1. Set the time on the CAM and CAS correctly first (see Set System Time, page 14-5)
2. Ensure you export the certificate from your CAM, save it on a machine accessible from your CAS, and import the exported certificate on the CAS, and repeat the process in reverse to ensure the CAS certificate also resides on the CAM.
3. Regenerate the certificate on the CAS using the correct IP address or domain.
4. Reboot the CAS.
5. Regenerate the certificate on the CAM using the correct IP address or domain.
6. Reboot the CAM.

Note If you check **`nslookup`** and **`date`** from the CAS, and both the DNS and TIME settings on the CAS are correct, this can indicate that the caCerts file on the CAS is corrupted. In this case Cisco recommends backing up the existing caCerts file from /usr/java/j2sdk1.4/lib/security/caCerts, then override it with the file from /perfigo/common/conf/caCerts, then perform "service perfigo restart" on the CAS.

Note If the error message on the client is "Clean Access Server is not properly configured, please report to your administrator," this typically is not a certificate issue but indicates that a default user login page has not been added to the CAM. See Add Default Login Page, page 5-3 for details.

For additional information, see also:

- Troubleshooting when Adding the Clean Access Server, page 2-8

- Agent Troubleshooting, page 11-36

Private Key in Clean Access Server Does Not Match the CA-Signed Certificate

This issue can arise if a new temporary certificate is generated but a CA-signed certificate is returned for the Certificate Signing Request (CSR) generated from a previous temporary certificate and Private Key pair.

For example, an administrator generates a CSR, backs up the Private Key, and then sends the CSR to a CA authority, such as VeriSign.

Subsequently, another administrator regenerates a temporary certificate after the CSR has been sent. When the CA-signed certificate is returned from the CA authority, the Private Key on which the CA-certificate is based no longer matches the one in the Clean Access Server.

To resolve this issue, re-import the old Private Key and then install the CA-signed certificate.

Regenerating Certificates for DNS Name Instead of IP

If planning to regenerate certificates based on the DNS name instead of the IP address of your servers:

- Make sure the CA-signed certificate you are importing is the one with which you generated the CSR and that you have NOT subsequently generated another temporary certificate. Generating a new temporary certificate will create a new private-public key combination. In addition, always export and save the Private Key when you are generating a CSR for signing (to have the Private Key handy).
- When importing certain CA-signed certificates, the system may warn you that you need to import the root certificate (the CA's root certificate) used to sign the CA-signed certificate, or the intermediate root certificate may need to be imported.
- Make sure there is a DNS entry in the DNS server.
- Make sure the DNS address in your Clean Access Server is correct.
- For High-Availability (failover) configurations, use the DNS name for the Service IP (virtual DNS).
- Cisco recommends rebooting when you generate a new certificate or import a CA-signed certificate.
- When using a DNS-based certificate, if it is not CA-signed, the user will simply be prompted to accept the certificate.

Disabling Administrator Prompt for Certificate on IE 8 and 9

If no certificates or only one certificate is installed in the personal store in Windows then there is an administrator prompt for certificate in IE9. The prompt can be disabled by setting the option on Internet Explorer.

To disable the prompt:

Step 1 Go to **Tools > Internet Options**.

Step 2 Click the the **Security** tab. Select a zone to view or change security settings (that the NAC Manager URL falls under).

Step 3 Click **Custom level** under Security level for this zone.

Step 4 **Enable** Don't prompt for client certificate selection when no certificates or only one certificate exists.

Certificate-Related Files

For troubleshooting purposes, Table 14-1 lists certificate-related files on the Clean Access Manager. For example, if the admin console becomes unreachable due to a mismatch of the CA-certificate/Private Key combination, these files may need to be modified directly in the file system of the Clean Access Manager.

Table 14-1 Clean Access Manager Certificate-Related Files

File	Description
/root/.tomcat.key	Private key
/root/.tomcat.crt	Certificate
/root/.tomcat.req	Certificate Signing Request
/root/.chain.crt	Intermediate certificate
/root/.perfigo/caCerts	The root CA bundle

For additional information on Clean Access Manager files, see Cisco NAC Appliance Log Files, page 13-11.

System Upgrade

In Cisco NAC Appliance Release 4.9 and later, you can perform system upgrades from Release 4.7(x) and 4.8(x) by uploading a .tar.gz upgrade file to the CAM/CAS and executing an upgrade script using the appliance's CLI. For complete upgrade details, including instructions for upgrading HA CASs and upgrades via SSH, refer to the "Upgrading" section of the corresponding *Release Notes for Cisco NAC Appliance*.

You can use the CAM web console to upload Release 4.9(x) .tar.gz upgrade files, and view upgrade logs and upgrade details.

Step 1 Choose **Administration > CCA Manager > Software Upload**.

Step 2 Download the .tar.gz upgrade image to your local machine from Cisco Software Download Site as described in the "Upgrading" section of the corresponding *Release Notes for Cisco NAC Appliance*.

a. In the **Software Upload** page**,** click **Browse** to navigate to the directory where you have stored the .tar.gz upgrade file.

b. Click **Upload**. After a brief time, the web console screen automatically refreshes, displaying the newly uploaded upgrade image and the date/time when it was uploaded to the CAM.

You can use the **Notes** link that appears after the image file name to view important information about the .tar.gz upgrade image.

Step 3 To view upgrade log information, click on the link under **List of Upgrade Logs** to launch a browser window displaying a brief summary of the upgrade process including the date and time the upgrade was performed.

Step 4 To view important upgrade process details, click on the link under **List of Upgrade Details** to launch a browser window displaying the details of the upgrade process, in the following format:

- State before upgrade
- Upgrade process details

- State after upgrade

It is normal for the "state before upgrade" to contain several warning/error messages (e.g. "INCORRECT"). The "state after upgrade" should be free of any warning or error messages.

Licensing

The Clean Access Manager and Clean Access Servers require a valid product license to function. The licensing model for Clean Access incorporates the FlexLM licensing standard.

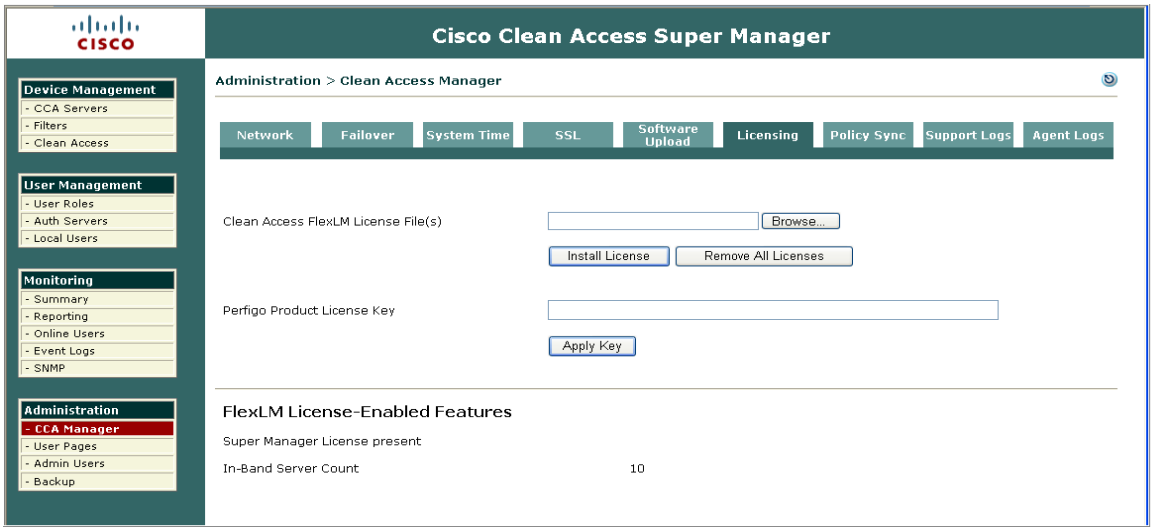
Note For step-by-step instructions on initially installing the Clean Access Manager license, as well as details on permanent, evaluation, and legacy licenses, see *Cisco NAC Appliance Service Contract / Licensing Support*.

Install FlexLM License for Clean Access Server:

Once the initial product license for the Clean Access Manager is installed, you can use the **Licensing** page to add or manage additional licenses (such as CAS licenses, or a second CAM license for HA-CAMs).

1. Go to **Administration > CCA Manager > Licensing**.

Figure 14-13 Licensing Page



2. In the **Clean Access Manager License File** field, browse to the license file for your Clean Access Server or Server bundle and click **Install License**. You will see a green confirmation text string at the top of the page if the license was installed successfully, as well as the CAS increment count (for example, "License added successfully. Out-of-Band Server Count is now 10.").

3. Repeat this step for each Clean Access Server license file you need to install (you should have received one license file per PAK submitted during customer registration). The status information at the bottom of the page will display total number of Clean Access Servers enabled per successful license file installation.

Note The Standby CAM does not read the License file till it becomes Active. Hence, the total number of CAS devices is not displayed in the Licensing page of the Standby CAM GUI.

Remove Product Licenses

1. Go to **Administration > CCA Manager > Licensing**.
2. Click the **Remove All Licenses** button to remove all FlexLM license files in the system.
3. The Clean Access Manager License Form will reappear in the browser, to prompt you to install a license file for the Clean Access Manager.

Note Until you enter the license file for the Clean Access Manager, you will not be redirected to the admin user login page of the web admin console.

Note

- You cannot remove individual FlexLM license files. To remove a file, you must remove all license files.
- Once installed, a permanent FlexLM license overrides an evaluation FlexLM license.
- Once installed, FlexLM licenses (either permanent or evaluation) override legacy license keys (even though the legacy key is still installed).
- When an evaluation FlexLM expires, or is removed, an existing legacy license key will again take effect.

Remove Legacy License Keys

1. Go to **Administration > CCA Manager > Licensing**.
2. To remove an old legacy license key (for releases prior to release 3.5), replace the license key in the **Perfigo Product License Key** field with a space (or any set of characters that are not the license string), then click **Apply Key**. This invalidates the license by replacing it whatever is entered so that the CAM does not recognize it as a valid license.

Policy Import/Export

The Policy Import/Export feature allows administrators to propagate device filters, traffic and remediation policies, and OOB port profiles from one CAM to several CAMs. You can define policies on a single CAM and configure it to be the Policy Sync Master. You can then configure up to a maximum of 10 CAMs or 10 CAM HA-pairs to be Policy Sync Receivers. You can export policies manually or schedule an Auto Policy Sync to occur once every *x* number of days.

A CAM can be either a Master or Receiver for Policy Sync, and only one Master CAM is allowed to push policies for a given set of Receivers. To perform Policy Sync, the Master and Receiver CAMs must authorize each other using the DN from the SSL certificate for each CAM or CAM HA-pair. For production deployments, CA-signed SSL certificates should be used. CAM HA-pairs will need an SSL certificate generated for the Service IP of the pair, with the DN from this certificate used to authorize each CAM in the HA pair for the Policy Sync configuration.

During Policy Sync, the Master configuration completely overrides (and clears) the existing Receiver configuration for the policies that are configured for Policy Sync, such as OOB profiles or user roles. Policies/configurations that are not subject to Policy Sync are otherwise left alone on the Receiver CAM after a Policy Sync.

Note
- All CAMs must run release 4.5 or later to enable Policy Sync.
- On CAM HA-pairs, Policy Sync settings are disabled for the Standby CAM.

Policy Sync Policies

Policy Sync enables the following global configurations to be propagated from a Master CAM.

- **Role-Based Policies**
  - User roles with associated global traffic control policies (IP-based, Host-based, L2 Ethernet) and session timers

    Note This includes customized policies and the Default Host Policies, Default L2 Policies from Cisco Updates that are on the Master CAM.

  - Global device filters with access type: Role or Check
  - Agent rules (Cisco and AV/AS), requirements, rule-requirement mappings, and role-requirement mappings

    Note This includes customized checks/rules and Cisco Checks & Rules and Supported AV/AS Product List (Windows & Macintosh) from Cisco Updates that are on the Master CAM and associated to rules/requirements.

- **Non Role-Based Policies**
  - Global device filters with access type: Allow, Deny or Ignore
- **OOB Policies** (excludes switch information (i.e. Device/SNMP))
  - Port Profiles

- VLAN Profiles

Note Cisco recommends that you configure auto update settings on the Master CAM (under **Device Management > Clean Access > Updates > Update**) to ensure the Master CAM has the latest Cisco Updates before you perform a Policy Sync.

Note Policy Sync exports all global device filters created on the Master CAM to the Receiver CAMs. Any MAC address which is in the Master CAM's global Device Filter list will be exported, including Cisco NAC Profiler generated filters. Refer to Global Device and Subnet Filtering, page 2-10 for additional details.

Note OOB policies should not be selected for Policy Sync if a Master is not configured for OOB, as this will clear any OOB policies on the Receiver CAM. Refer to Chapter 3, "Switch Management: Configuring Out-of-Band Deployment" for details on OOB.

Policies Excluded from Policy Sync

Policies/configurations that are not listed under Policy Sync Policies, page 14-28 are not subject to Policy Sync and are otherwise left alone on the Receiver CAM after a Policy Sync. The following non-exhaustive list describes the kinds of policies/configurations that are **not included** for Policy Sync:

- Cisco NAC Appliance Agents. The Master and Receiver CAMs retain the Agent versions and Agent download and distribution policies they already have. You will still need to require use of the Agent for a role and operating system (e.g. Agent Login/Distribution pages) on each CAM.
- Local configuration on the Receiver CAMs such as CAS-specific traffic policies or device filters. Local policies stay the same on the Receiver CAM and are not removed after a Policy Sync.
- OOB switch configurations such as **Device** Profiles and **SNMP Receiver** settings.
- Agent Updates for Cisco NAC Appliance Agents, OS Detection Fingerprinting, and Switch OIDs
- User Login pages, Local Users, or Bandwidth policies associated with a user role.
- Subnet filters
- Authentication server configurations
- Certified Device List or Timers
- Network Scanning (Nessus) configuration

Example Scenarios

Master is configured, Receiver is not configured:

- For the Master CAM:
  - Role A is configured with traffic and posture assessment policies
  - Role A requires use of the Agent
- For the Receiver CAM:
  - No roles are configured

- After a Policy Sync:
  - For the Receiver CAM:

    Role A is created and configured with traffic and posture assessment policies from the Master CAM.

    The administrator still needs to map the Agent Login settings to require use of the Agent for Role A.

Master is configured, Receiver is configured:

- For the Master CAM:
  - Role A is configured with traffic and posture assessment policies
  - Role A requires use of the Agent for Windows ALL.
- For the Receiver CAM:
  - Role A is configured with different traffic and posture assessment policies
  - Role A requires use of the Agent for Vista Only.
  - Role B is configured
- After a Policy Sync:
  - For the Receiver CAM:

    Role A is configured with traffic and posture assessment policies from the Master CAM

    Role A requires use of the Agent for Vista only.

    Role B is removed.

Policy Sync Configuration Summary

Step 1 Before You Start, page 14-30

Step 2 Enable Policy Sync on the Master, page 14-31

Step 3 Configure the Master, page 14-32

Step 4 Enable Policy Sync on the Receiver, page 14-34

Step 5 Configure the Receiver, page 14-35

Step 6 Perform Policy Sync, page 14-36

Step 7 View History Logs, page 14-39

Step 8 Troubleshooting Manual Sync Errors, page 14-41

Before You Start

Step 1 Make sure all CAMs to be used for Policy Sync (Master and Receivers):

- Fulfill the Release 4.5 upgrade requirements and are running release 4.5 (or later)
- Have a properly configured SSL certificate. For production deployments, make sure SSL certificates are CA-signed.

Step 2 Identify the CAM you want to designate as the Policy Sync Master.

Step 3 Make sure the following are properly configured on the designated Master CAM before you begin:

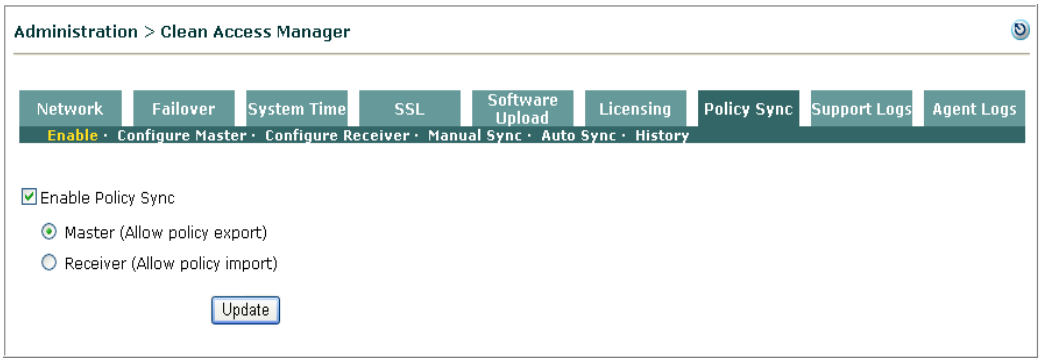
- Cisco NAC Appliance Updates
- User roles
- Traffic policies and session timers for the user roles
- Agent rules, requirements, rule-requirement mappings and requirement-role mappings
- Device filters (role/check and allow/deny/ignore)
- For OOB deployments, make sure the Master CAM is configured properly for OOB, including Port and VLAN profile configuration. If the Master CAM is not configured for OOB, but a Receiver CAM is, make sure not to push OOB policies from the Master CAM, or you will lose the OOB policies on the Receiver.
- Agent Login/Distribution/Installation properties for Master CAM user roles/operating systems. Note that these settings are not exported by Policy Sync. You will need to configure these settings on the Receiver CAMs for any new roles added by Policy Sync.

Step 4 Verify that the policies on the CAMs you want to designate as Receivers can be overwritten by Policy Sync.

Enable Policy Sync on the Master

Step 1 From the web console of the Clean Access Manager you want to designate as the Policy Sync Master, go to **Administration > CCA Manager > Policy Sync > Enable** (Figure 14-14).

Figure 14-14 Enabling Policy Sync on the Master CAM



Step 2 Click the checkbox for **Enable Policy Sync**.

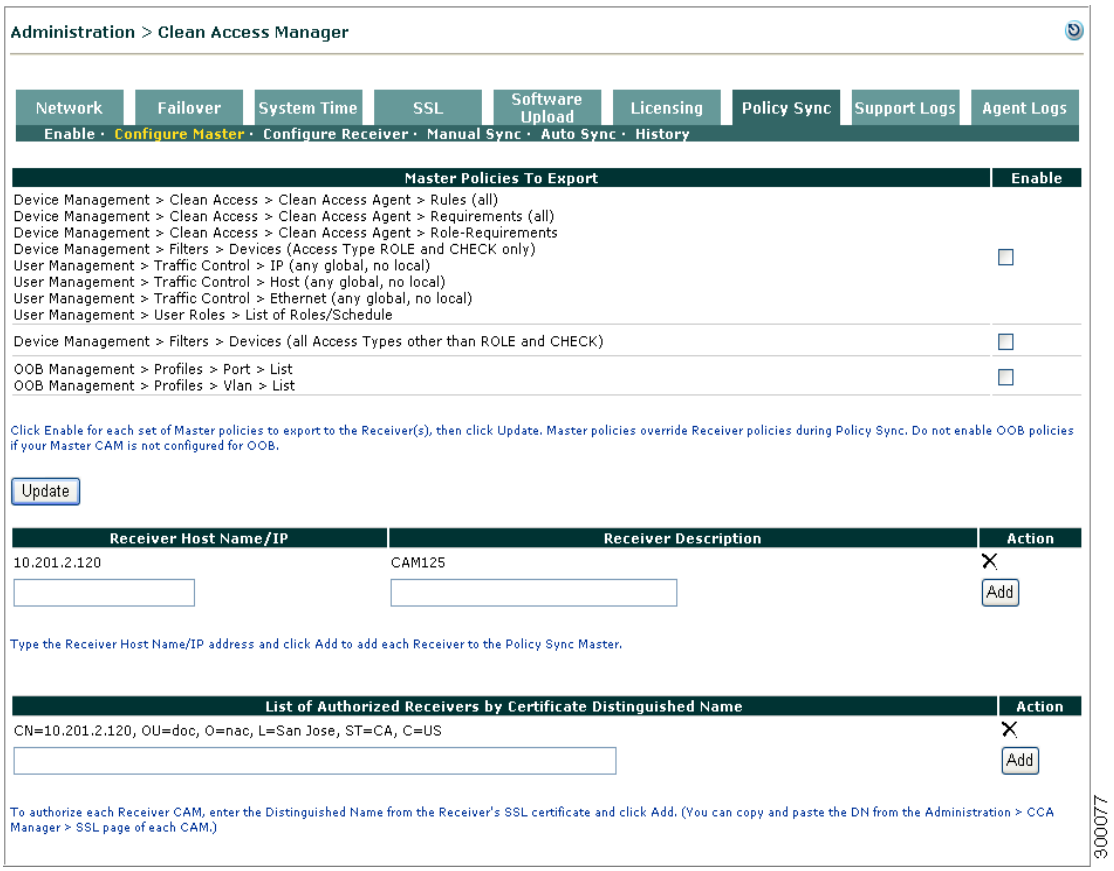
Step 3 Click the radio button for **Master (Allow policy export)**.

Step 4 Click **Update**. This sets the current CAM as the Policy Sync Master and enables the **Configure Master**, **Manual Sync** and **Auto Sync** pages for this CAM (disabling the **Configure Receiver** page).

Configure the Master

Step 1 From the **Policy Sync** tab, click the **Configure Master** link (Figure 14-15).

Figure 14-15 Configure Master


Administration > Clean Access Manager
Network
Failover
System Time
SSL
Software Upload
Licensing
Policy Sync
Support Logs
Agent Logs
Enable · Configure Master · Configure Receiver · Manual Sync · Auto Sync · History
Master Policies To Export
Enable
Device Management > Clean Access > Clean Access Agent > Rules (all)
Device Management > Clean Access > Clean Access Agent > Requirements (all)
Device Management > Clean Access > Clean Access Agent > Role-Requirements
Device Management > Filters > Devices (Access Type ROLE and CHECK only)
User Management > Traffic Control > IP (any global, no local)
User Management > Traffic Control > Host (any global, no local)
User Management > Traffic Control > Ethernet (any global, no local)
User Management > User Roles > List of Roles/Schedule
Device Management > Filters > Devices (all Access Types other than ROLE and CHECK)
OOB Management > Profiles > Port > List
OOB Management > Profiles > Vlan > List
Click Enable for each set of Master policies to export to the Receiver(s), then click Update. Master policies override Receiver policies during Policy Sync. Do not enable OOB policies if your Master CAM is not configured for OOB.
Update
Receiver Host Name/IP
Receiver Description
Action
10.201.2.120
CAM125
Add
Type the Receiver Host Name/IP address and click Add to add each Receiver to the Policy Sync Master.
List of Authorized Receivers by Certificate Distinguished Name
Action
CN=10.201.2.120, OU=doc, O=nac, L=San Jose, ST=CA, C=US
Add
To authorize each Receiver CAM, enter the Distinguished Name from the Receiver's SSL certificate and click Add. (You can copy and paste the DN from the Administration > CCA Manager > SSL page of each CAM.)
300077

Step 2 Click the checkbox for each set of policies you want to include in the Policy Sync:

- **Role-based:**

  Device Management > Clean Access > Clean Access Agent > Rules (all)
  Device Management > Clean Access > Clean Access Agent > Requirements (all)
  Device Management > Clean Access > Clean Access Agent > Role-Requirements
  Device Management > Filters > Devices (Access Type ROLE and CHECK only)
  User Management > Traffic Control > IP (any global, no local)
  User Management > Traffic Control > Host (any global, no local)
  User Management > Traffic Control > Ethernet (any global, no local)
  User Management > User Roles > List of Roles/Schedule

- **Non-role-based Device Filters:**

  Device Management > Filters > Devices (all Access Types other than ROLE and CHECK)

- **OOB Port and VLAN Profiles:**

  OOB Management > Profiles > Port > List

  OOB Management > Profiles > VLAN > List

Step 3 Click the **Update** button. You must click **Update** each time you change the set of policies to include for Policy Sync.

Step 4 Add each Receiver to the Master as follows:

a. In the **Receiver Host Name/IP** text box, type the domain name or IP address of the receiver CAM. For HA-CAMs, type the Service IP of the CAM HA pair.

b. Type an optional **Receiver Description**

c. Click the **Add** button. (To delete a Receiver, you can click the "X" icon in the **Action** column.)

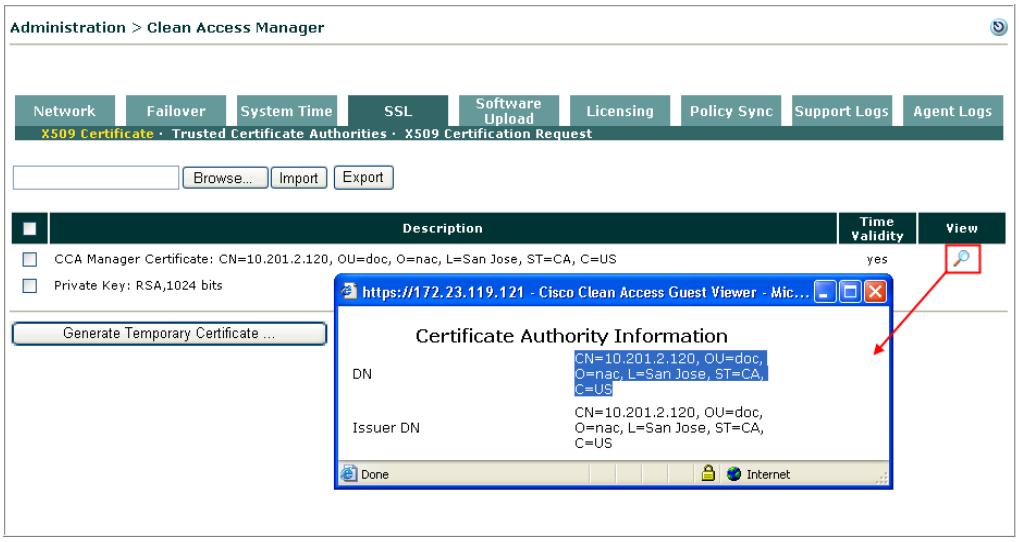
Note Policy Sync supports a maximum of 10 CAMs or 10 HA-CAM pairs.

Step 5 Authorize each Receiver CAM as described in the following steps. Authorization allows verification of the Distinguished Name on the SSL certificates of the Master and Receiver CAMs to ensure the communication between them is secure and limited to the respective parties.

a. Obtain the DN of the Receiver CAM as follows:

- navigate to **Administration > CCA Manager > SSL > x509 Certificate** on the Receiver CAM console
- click the **View** button to bring up the **Certificate Authority Information** dialog.
- copy the **DN** entry (Figure 14-16).

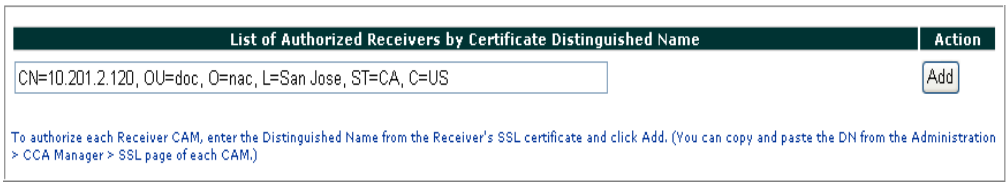
Figure 14-16 Copying the DN Information from the Receiver CAM



b. On the Master CAM, navigate to **Administration > CCA Manager > Policy Sync > Configure Master**

c. Paste the DN from the SSL certificate of the Receiver CAM into the **List of Authorized Receivers by Certificate Distinguished Name** text box (Figure 14-17).

Figure 14-17 Authorizing the Receiver on the Master CAM


List of Authorized Receivers by Certificate Distinguished Name
Action
CN=10.201.2.120, OU=doc, O=nac, L=San Jose, ST=CA, C=US
Add
To authorize each Receiver CAM, enter the Distinguished Name from the Receiver's SSL certificate and click Add. (You can copy and paste the DN from the Administration > CCA Manager > SSL page of each CAM.)
300101

d. Click the **Add** button. (To delete a Receiver, you can click the "X" icon in the **Action** column.)

Note Policy Sync supports a maximum of 10 CAMs or 10 HA-CAM pairs.

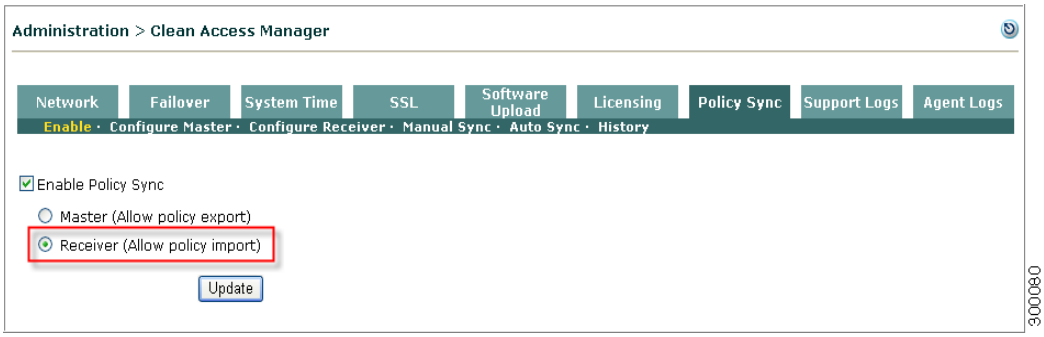
Note Authorization must be configured on both the Master and Receiver CAMs for the Master to successfully push policies and for the Receiver to accept them.

Enable Policy Sync on the Receiver

A CAM configured as a Policy Sync Receiver is distinguished by a red-colored product banner, and Master CAM settings are disabled for the Receiver CAM. The red banner is intended to warn administrators not to change any policies on the Receiver CAM for which Policy Sync applies.

Step 1 From the web console of the Receiver CAM, go to **Administration > CCA Manager > Policy Sync > Enable** (Figure 14-18).

Figure 14-18 Enabling Policy Sync on the Receiver CAM

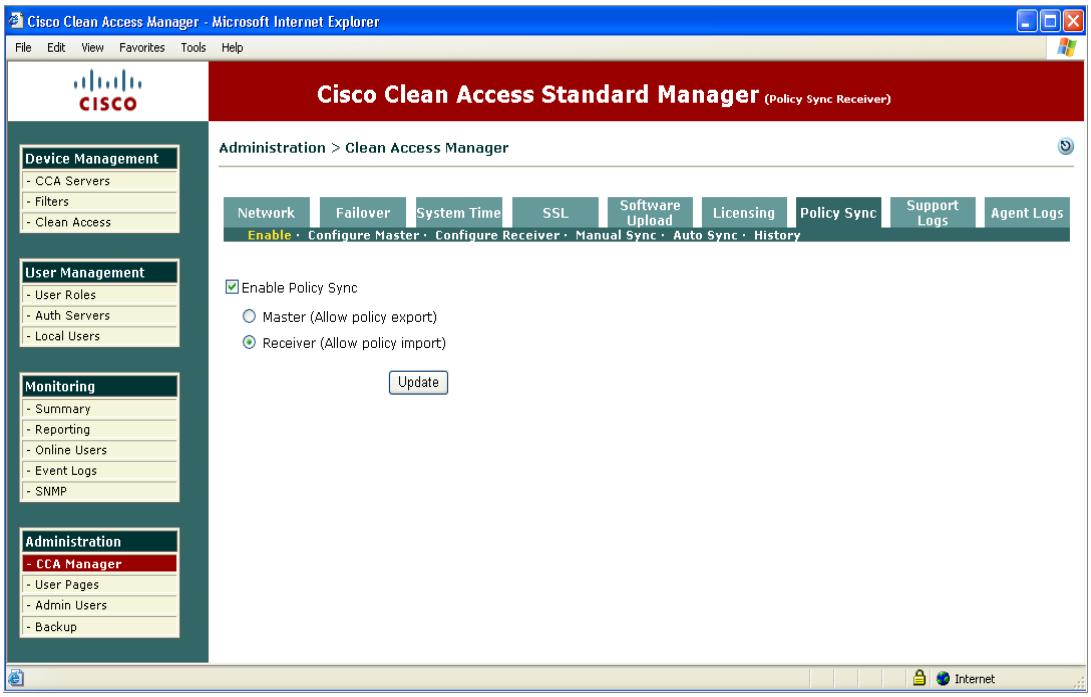


Step 2 Click the checkbox for **Enable Policy Sync**.

Step 3 Click the radio button for **Receiver (Allow policy import)**.

Step 4 Click **Update**. This sets the current CAM as the Policy Sync Receiver. This labels the CAM as "Policy Sync Receiver" and changes the color of the web console product banner to red, as shown in Figure 14-19. It also enables the **Configure Receiver** page for this CAM and disables the **Configure Master, Manual Sync** and **Auto Sync** pages.

Figure 14-19 Policy Sync Receiver (Displays Red Product Banner)

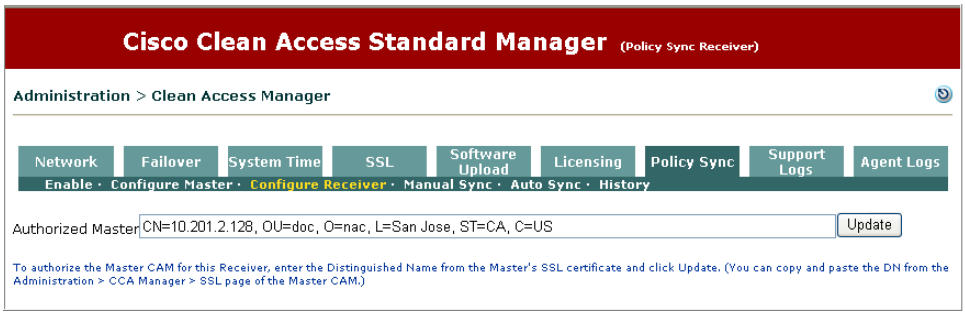


Configure the Receiver

This step consists of authorizing the Master CAM on the Receiver CAM.

Step 1 From the web console of the Receiver CAM, go to **Administration > CCA Manager > Policy Sync > Configure Receiver** (Figure 14-20).

Figure 14-20 Configure Receiver


Cisco Clean Access Standard Manager (Policy Sync Receiver)
Administration > Clean Access Manager
Network Failover System Time SSL Software Upload Licensing Policy Sync Support Logs Agent Logs
Enable · Configure Master · Configure Receiver · Manual Sync · Auto Sync · History
Authorized Master CN=10.201.2.128, OU=doc, O=nac, L=San Jose, ST=CA, C=US
Update
To authorize the Master CAM for this Receiver, enter the Distinguished Name from the Master's SSL certificate and click Update. (You can copy and paste the DN from the Administration > CCA Manager > SSL page of the Master CAM.)
300099

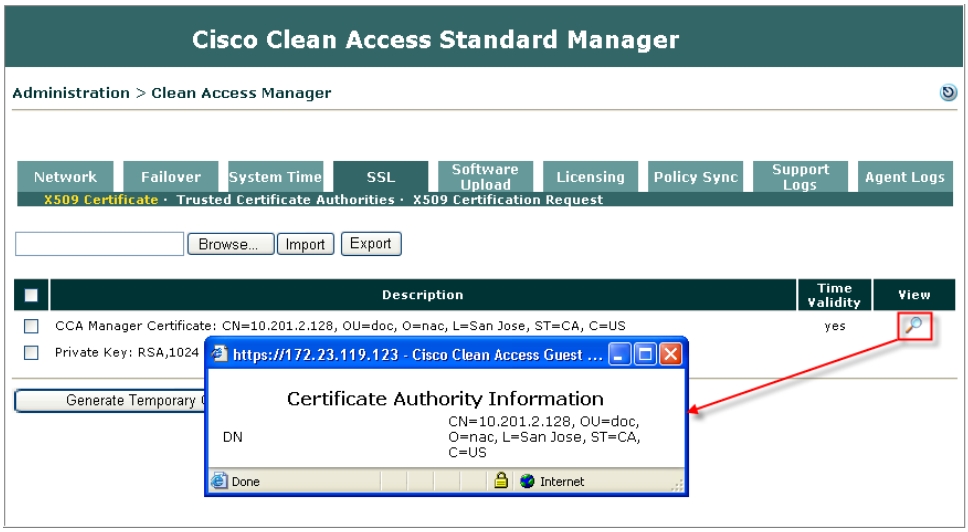
Step 2 Authorize the Master CAM with the following steps:

a. Obtain the DN of the Master CAM as follows:

– Navigate to **Administration > CCA Manager > SSL > x509 Certificate** on the Master CAM console

- Click the **View** icon to bring up the **Certificate Authority Information** dialog
- Copy the **DN** entry (Figure 14-21).

Figure 14-21 Copying the DN Information from the Master CAM



b. On the Receiver CAM, navigate to **Administration > CCA Manager > Policy Sync > Configure Receiver**.

c. Paste the DN from the SSL certificate of the Master CAM in the **Authorized Master** text box (Figure 14-20).

Step 3 Click **Update**.

Perform Policy Sync

You can schedule automatic sync of policies at specific time interval once every *x* number of days. You can also manually sync policies at any time. You must be logged in as a Full-Control Admin user to the Master CAM in order to perform automated or manual policy sync.

The Master configuration completely overrides (and clears) the existing Receiver configuration for the policies that are configured for Policy Sync, such as OOB profiles or user roles. Policies/configurations that are not subject to Policy Sync are otherwise left alone on the Receiver CAM after a Policy Sync.

Note that when Rules are pushed during a Policy Sync, all associated Checks are automatically pushed as well.

Policy Sync results (manual or auto) are logged on the **History** page for each Master and Receiver CAM. In addition, Auto Sync results are logged in the Master CAM's **Event Log**s.

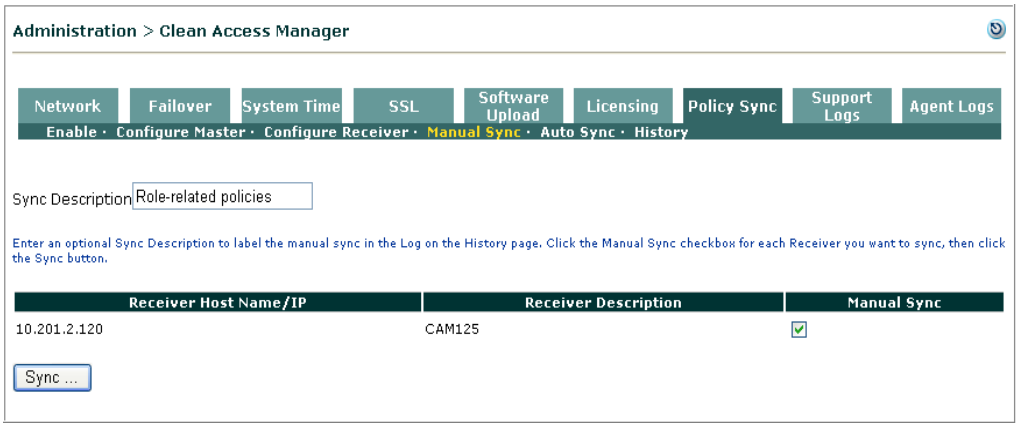
Note The Cisco Updates on the Master override any updates on the Receiver. Therefore, Cisco recommends that you configure auto update settings on the Master (under **Device Management > Clean Access > Updates > Update**) to ensure the Master has the latest Cisco Updates before performing a Policy Sync.

Perform Manual Sync

Step 1 On the Master CAM, make sure only the policies you want to manually sync are enabled on **Configure Master** (Figure 14-15) page. Make sure to click the **Update** button if changing the settings.

Step 2 On the Master CAM go to **Administration > CCA Manager > Policy Sync > Manual Sync** (Figure 14-22)

Figure 14-22 Manual Sync


Administration > Clean Access Manager
Network
Failover
System Time
SSL
Software Upload
Licensing
Policy Sync
Support Logs
Agent Logs
Enable · Configure Master · Configure Receiver · Manual Sync · Auto Sync · History
Sync Description Role-related policies
Enter an optional Sync Description to label the manual sync in the Log on the History page. Click the Manual Sync checkbox for each Receiver you want to sync, then click the Sync button.
Receiver Host Name/IP
Receiver Description
Manual Sync
10.201.2.120
CAM125
Sync ...
300079

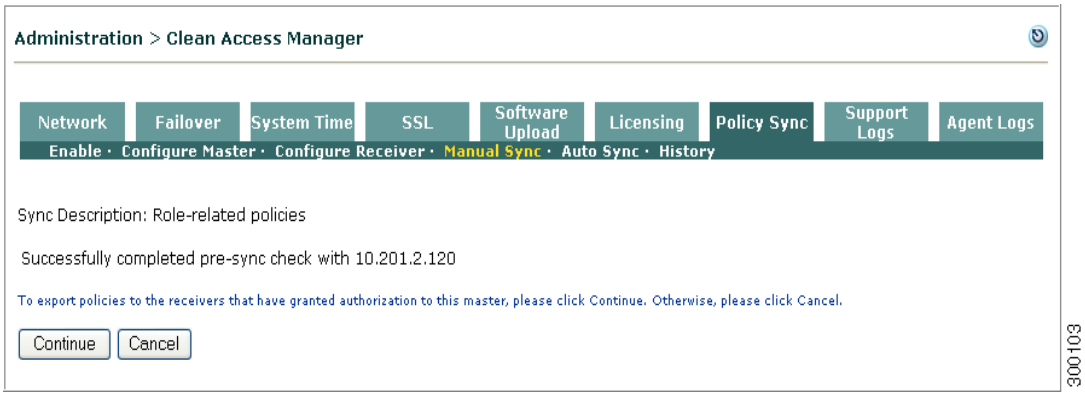
Step 3 All configured Policy Receivers appear under the **Receiver Host Name/IP** column on the page.

Step 4 In the **Sync Description** text box, type an optional description for the manual sync to be performed. The description labels the manual sync in the Logs on the **History** page.

Step 5 Click the **Manual Sync** checkbox for each Receiver CAM to which you want to export polices.

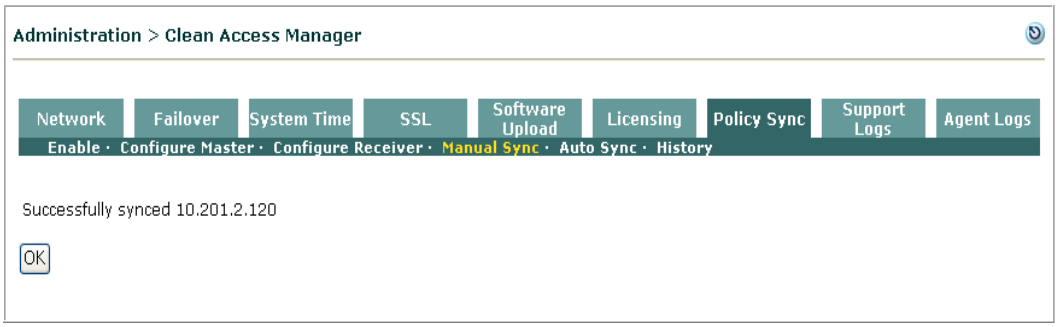
Step 6 Click the **Sync** button. The pre-sync check screen appears (Figure 14-23).

Figure 14-23 Manual Sync (Authorization Check)



Step 7 Click the **Continue** button to complete the manual Policy Sync. If successful, the following screen appears (Figure 14-24).

Figure 14-24 Successful Manual Sync



Step 8 Click **OK** to return to the main screen.

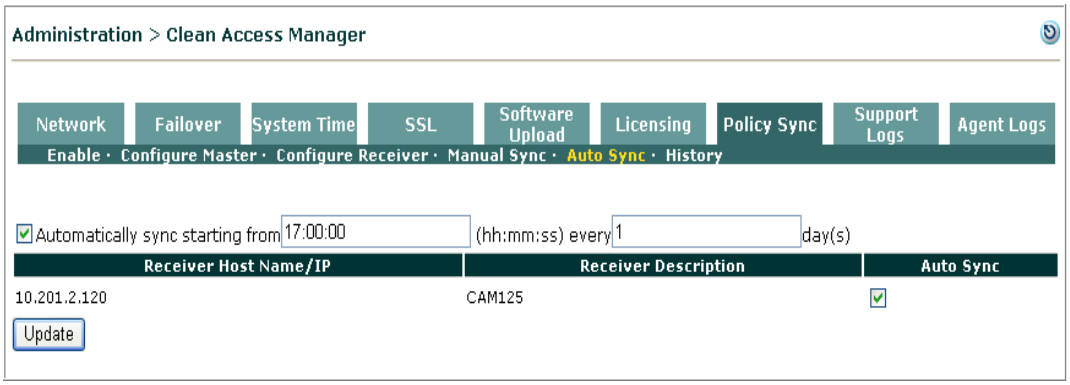
Perform Auto Sync

Note Cisco strongly recommends performing a Manual Sync and verifying that it is working successfully before enabling Auto Sync between your Clean Access Managers.

Step 1 On the Master CAM, make sure only the policies you want to enable for auto sync are selected on the **Configure Master** page (Figure 14-15). Make sure to click the **Update** button if changing the settings.

Step 2 On the Master CAM, go to **Administration > CCA Manager > Policy Sync > Auto Sync** (Figure 14-25)

Figure 14-25 Auto Sync



Step 3 The list of configured Receivers appears under the **Receiver Host Name /IP** column on the page.

Step 4 Click the checkbox for **Automatically sync starting from**[]. In the adjoining text box, type the initial time to start and repeat the auto policy sync in **hh:mm:ss** format (e.g. 22:00:00)

Step 5 In the **every [] day(s)** text box, type the number of days after which to repeat the auto synchronization. The minimal interval is 1 for 1 day.

Step 6 Click the **Auto Sync** checkbox for each Receiver CAM to which you want to export polices.

Step 7 Click the **Update** button to set the schedule. The Master CAM will perform Auto Policy Sync at the interval you specified and will display log results on the **History** page as "**Auto sync**" and in the Master CAM's Event Logs.

Verify Policy Sync

Step 1 Go to the Receiver CAM and confirm the Master policies are pushed via Policy Sync.

Step 2 If there are issues, you can troubleshoot further:

- View History Logs, page 14-39
- Troubleshooting Manual Sync Errors, page 14-41

View History Logs

Details of each manual and automated Policy Sync are logged on the **History** page for both the Master and Receiver CAMs. Each Master and Receiver CAM keeps up to 300 entries of History logs.

In addition, Auto Sync is logged in the Master CAM's **Event Logs** when Auto Sync is enabled. The result of each Auto Sync is logged as an Administration event under **Monitoring > Event Logs** in addition to the **Policy Sync > History** logs. Refer to Interpreting Event Logs, page 13-4 for additional information.

Step 1 To view logs, go to **Administration > CCA Manager > Policy Sync > History** for the Master (Figure 14-26) or Receiver CAM (Figure 14-27).

Step 2 The columns displayed are as follows:

- **Sync ID**—unique ID for the policy sync session, with format: [start time on Master]_[random number].[an integer for each Receiver, starting from 0 (with sequence 1, 2, 3, and so on)].
- **Master DN—[THIS CAM]** if this is the Master or the Master's IP/DN.
- **Receiver DN—[THIS CAM]** if this is the Receiver or the Receiver's IP/DN.
- **Status**—"succeeded" or "failed". Policy Sync failure means there is no transmission of policies from Master to Receiver, and no changes to the database for either CAM.
- **Start Time/End Time**—Duration of the policy sync session.
- **Description**—labelled "**Auto sync"** or blank for manual sync, unless a description is entered.
- **Log**—click the magnifying glass icon to view the individual log files (example Master: Figure 14-28) (example Receiver: Figure 14-29)
- **Action**—Click the "X" icon to remove this log.

Figure 14-26 History Logs for Master CAM

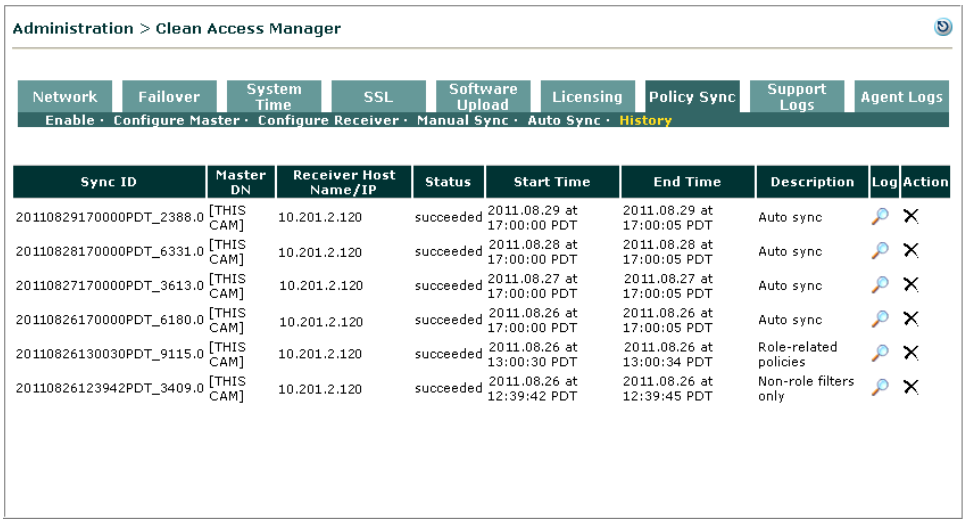

Administration > Clean Access Manager
Network
Failover
System Time
SSL
Software Upload
Licensing
Policy Sync
Support Logs
Agent Logs
Enable · Configure Master · Configure Receiver · Manual Sync · Auto Sync · History
Sync ID
Master DN
Receiver Host Name/IP
Status
Start Time
End Time
Description
Log
Action
20110829170000PDT_2388.0 [THIS CAM] 10.201.2.120 succeeded 2011.08.29 at 17:00:00 PDT 2011.08.29 at 17:00:05 PDT Auto sync
20110828170000PDT_6331.0 [THIS CAM] 10.201.2.120 succeeded 2011.08.28 at 17:00:00 PDT 2011.08.28 at 17:00:05 PDT Auto sync
20110827170000PDT_3613.0 [THIS CAM] 10.201.2.120 succeeded 2011.08.27 at 17:00:00 PDT 2011.08.27 at 17:00:05 PDT Auto sync
20110826170000PDT_6180.0 [THIS CAM] 10.201.2.120 succeeded 2011.08.26 at 17:00:00 PDT 2011.08.26 at 17:00:05 PDT Auto sync
20110826130030PDT_9115.0 [THIS CAM] 10.201.2.120 succeeded 2011.08.26 at 13:00:30 PDT 2011.08.26 at 13:00:34 PDT Role-related policies
20110826123942PDT_3409.0 [THIS CAM] 10.201.2.120 succeeded 2011.08.26 at 12:39:42 PDT 2011.08.26 at 12:39:45 PDT Non-role filters only
300104

Figure 14-27 History Logs for Policy Sync Receiver

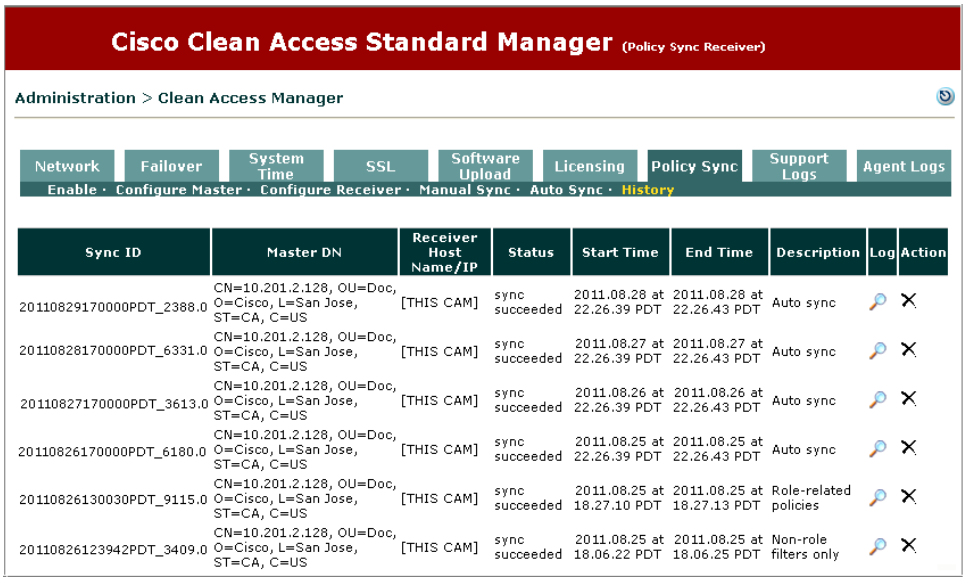

Cisco Clean Access Standard Manager (Policy Sync Receiver)
Administration > Clean Access Manager
Network
Failover
System Time
SSL
Software Upload
Licensing
Policy Sync
Support Logs
Agent Logs
Enable · Configure Master · Configure Receiver · Manual Sync · Auto Sync · History
Sync ID
Master DN
Receiver Host Name/IP
Status
Start Time
End Time
Description
Log
Action
20110829170000PDT_2388.0 CN=10.201.2.128, OU=Doc, O=Cisco, L=San Jose, ST=CA, C=US [THIS CAM] sync succeeded 2011.08.28 at 22.26.39 PDT 2011.08.28 at 22.26.43 PDT Auto sync
20110828170000PDT_6331.0 CN=10.201.2.128, OU=Doc, O=Cisco, L=San Jose, ST=CA, C=US [THIS CAM] sync succeeded 2011.08.27 at 22.26.39 PDT 2011.08.27 at 22.26.43 PDT Auto sync
20110827170000PDT_3613.0 CN=10.201.2.128, OU=Doc, O=Cisco, L=San Jose, ST=CA, C=US [THIS CAM] sync succeeded 2011.08.26 at 22.26.39 PDT 2011.08.26 at 22.26.43 PDT Auto sync
20110826170000PDT_6180.0 CN=10.201.2.128, OU=Doc, O=Cisco, L=San Jose, ST=CA, C=US [THIS CAM] sync succeeded 2011.08.25 at 22.26.39 PDT 2011.08.25 at 22.26.43 PDT Auto sync
20110826130030PDT_9115.0 CN=10.201.2.128, OU=Doc, O=Cisco, L=San Jose, ST=CA, C=US [THIS CAM] sync succeeded 2011.08.25 at 18.27.10 PDT 2011.08.25 at 18.27.13 PDT Role-related policies
20110826123942PDT_3409.0 CN=10.201.2.128, OU=Doc, O=Cisco, L=San Jose, ST=CA, C=US [THIS CAM] sync succeeded 2011.08.25 at 18.06.22 PDT 2011.08.25 at 18.06.25 PDT Non-role filters only
300105

Figure 14-28 Log File for Master

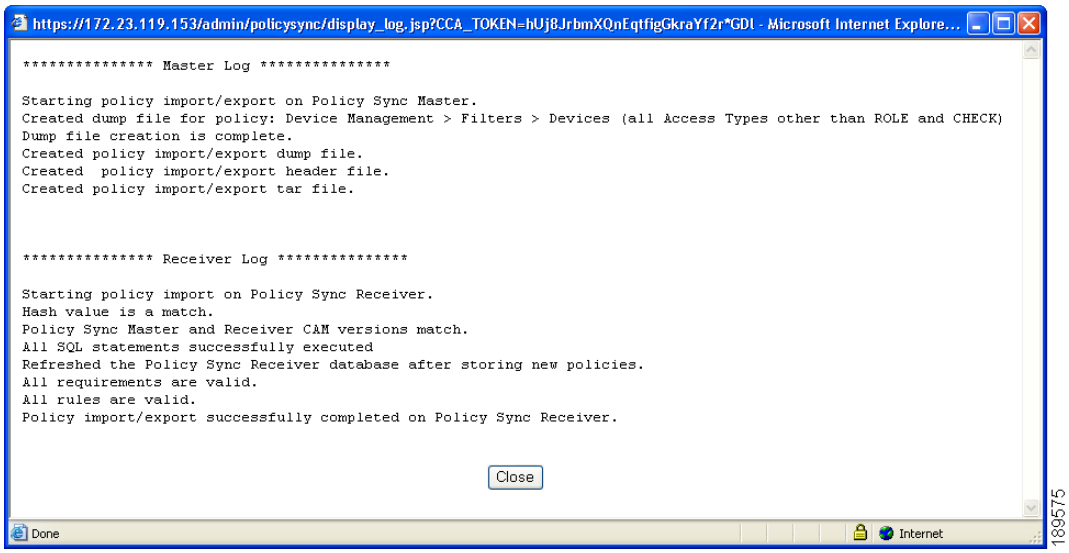
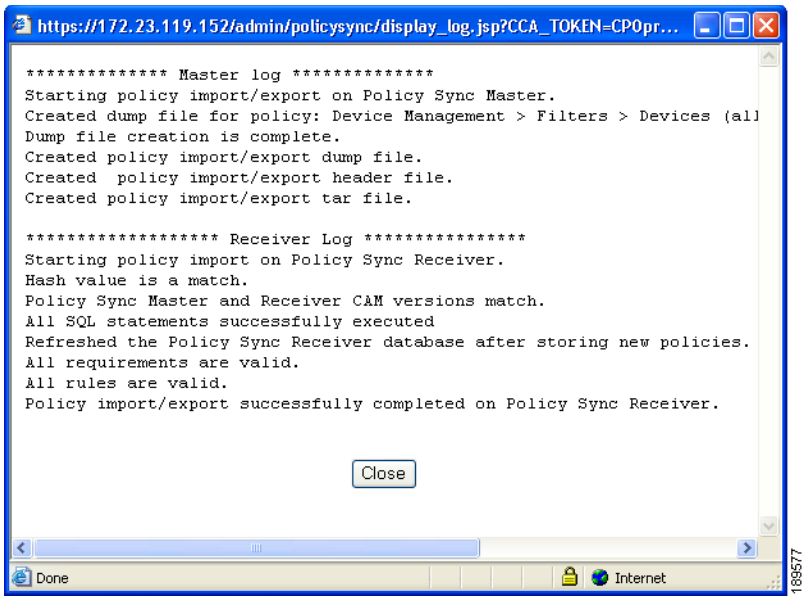

https://172.23.119.153/admin/policysync/display_log.jsp?CCA_TOKEN=hUj8JrbmXQnEqtfigGkraYf2r*GDl - Microsoft Internet Explore...
********** Master Log **********
Starting policy import/export on Policy Sync Master.
Created dump file for policy: Device Management > Filters > Devices (all Access Types other than ROLE and CHECK)
Dump file creation is complete.
Created policy import/export dump file.
Created policy import/export header file.
Created policy import/export tar file.
********** Receiver Log **********
Starting policy import on Policy Sync Receiver.
Hash value is a match.
Policy Sync Master and Receiver CAM versions match.
All SQL statements successfully executed
Refreshed the Policy Sync Receiver database after storing new policies.
All requirements are valid.
All rules are valid.
Policy import/export successfully completed on Policy Sync Receiver.
Close
Done
Internet
189575

Figure 14-29 Log File for Receiver


https://172.23.119.152/admin/policysync/display_log.jsp?CCA_TOKEN=CPOpr...
********** Master log **********
Starting policy import/export on Policy Sync Master.
Created dump file for policy: Device Management > Filters > Devices (all
Dump file creation is complete.
Created policy import/export dump file.
Created policy import/export header file.
Created policy import/export tar file.
********** Receiver Log **********
Starting policy import on Policy Sync Receiver.
Hash value is a match.
Policy Sync Master and Receiver CAM versions match.
All SQL statements successfully executed
Refreshed the Policy Sync Receiver database after storing new policies.
All requirements are valid.
All rules are valid.
Policy import/export successfully completed on Policy Sync Receiver.
Close
Done
Internet
189577

Troubleshooting Manual Sync Errors

Failed sanity check with [x.x.x.x]. Receiver denied access. This CAM is not authorized as Policy Sync Master.

This message displays on the Master CAM if the Receiver does not have the Master's DN configured or if the Master's DN is misconfigured on the **Configure Receiver** page.

To resolve this, navigate to **Administration > CCA Manager > Policy Sync > Configure Receiver** on the Receiver CAM and ensure the Master's DN is present and/or configured correctly.

Failed sanity check with [x.x.x.x]. The certificate's subject DN of this receiver is not authorized.

This message displays on the Master CAM if the Master does not have the Receiver DN configured or if the Receiver's DN is misconfigured under Configure Master page.

To resolve this, navigate to **Administration > CCA Manager > Policy Sync > Configure Master** on the Master CAM and ensure the Receiver's DN is present and/or configured correctly in the **List of Authorized Receivers by Certificate Distinguished Name**.

Failed sanity check with [x.x.x.x]. This host is not configured as policy sync receiver.

This message displays on the Master CAM if Policy Sync is not enabled on the Receiver.

To resolve this, Enable Policy Sync on the Receiver.

Support Logs

The **Support Logs** page on the Clean Access Manager is intended to facilitate TAC support of customer issues. The **Support Logs** page allows administrators to combine a variety of system logs (such as information on open files, open handles, and packages) into one tarball that can be sent to TAC to be included in the support case. Administrators should download these support logs when sending their customer support request.

The **Support Logs** pages on the CAM web console provide web page controls to configure the level of log detail recorded for troubleshooting purposes in **/perfigo/control/tomcat/logs/nac_manager.log**. These web controls are intended as convenient alternative to using the CLI `loglevel` command and parameters in order to gather system information when troubleshooting. Note that the log level configured on the Support Logs page does not affect the CAM's **Monitoring > Event Log** page display.

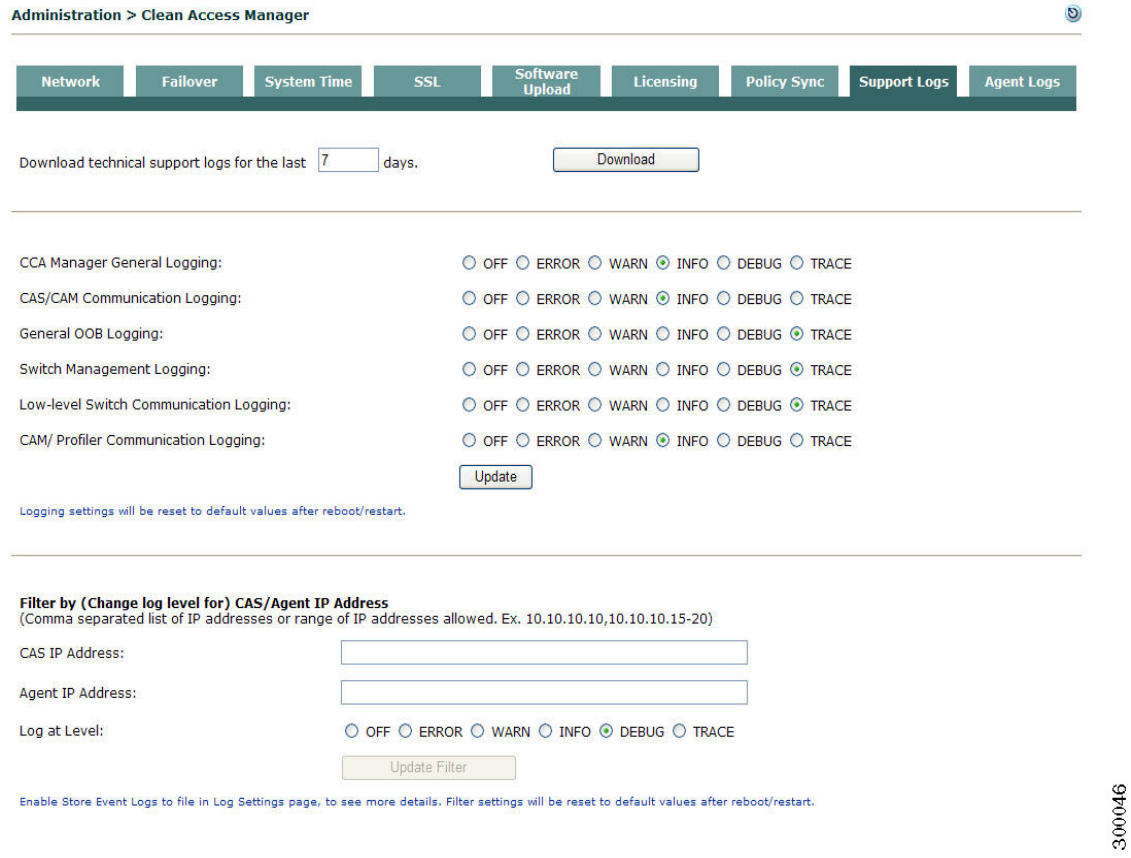
For normal operation, the log level should always remain at the default setting (**INFO**). The log level is only changed temporarily for a specific troubleshooting time period—typically at the request of the customer support/TAC engineer. In most cases, the setting is switched from **INFO** to **DEBUG** or **TRACE** for a specific interval, then reset to **INFO** after data is collected. Note that once you reboot the CAM, or perform the `service perfigo restart` command, the log level returns to the default setting (**INFO**).

Caution Cisco recommends using the **DEBUG** and **TRACE** options only temporarily for very specific issues. Although the CAM records logging information and stores them in a series of nine 20MB files before discarding any old logs, the large amount of logging information can cause the CAM to run out of available log storage space in a relatively short amount of time.

To Download CAM Support Logs:

Step 1 Go to **Administration > CCA Manager > Support Logs**.

Figure 14-30 Support Logs


Administration > Clean Access Manager
Network
Failover
System Time
SSL
Software Upload
Licensing
Policy Sync
Support Logs
Agent Logs
Download technical support logs for the last 7 days.
Download
CCA Manager General Logging:
CAS/CAM Communication Logging:
General OOB Logging:
Switch Management Logging:
Low-level Switch Communication Logging:
CAM/ Profiler Communication Logging:
OFF ERROR WARN INFO DEBUG TRACE
Update
Logging settings will be reset to default values after reboot/restart.
Filter by (Change log level for) CAS/Agent IP Address
(Comma separated list of IP addresses or range of IP addresses allowed. Ex. 10.10.10.10,10.10.10.15-20)
CAS IP Address:
Agent IP Address:
Log at Level:
Update Filter
Enable Store Event Logs to file in Log Settings page, to see more details. Filter settings will be reset to default values after reboot/restart.
300046

Step 2 Specify the number of days of debug messages to include in the file you will download for your Cisco customer support request.

Step 3 Click the **Download** button to download the **cam_logs.<cam-ip-address>.tar.gz** file to your local computer.

Step 4 Send this .tar.gz file with your customer support request.

Note To retrieve the compressed support logs file for the Clean Access Server, log in to the CAS web console and go to **Monitoring > Support Logs**. See the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)* for details.

To Change the Loglevel for CAM Logs:

Step 1 Go to **Administration > CCA Manager > Support Logs**.

Step 2 Choose the CAM log category to change:

- **CCA Manager General Logging**: This category contains the majority of logging events for the system. Any log event not contained in the other four categories listed below will be found under **CCA Manager General Logging** (e.g. authentication failures).
- **CAS/CAM Communication Logging**: This category contains CAM/CAS configuration or communication errors, for example, if the CAM's attempt to publish information to the CAS fails, the event will be logged.
- **General OOB Logging**: This category contains general OOB errors that may arise from incorrect settings on the CAM, for example, if the system cannot process an SNMP linkup trap from a switch because it is not configured on the CAM or is overloaded.
- **Switch Management Logging**: This category contains generic SNMP errors that can arise from the CAM directly communicating with the switch, for example, if the CAM receives an SNMP trap for which the community string does not match.
- **Low-level Switch Communication Logging**: This category contains OOB errors for specific switch models.
- **CAM/ Profiler Communication Logging**: This category contains the logs/errors at different levels of the synchronization of the Cisco ISE Profiler with NAC Appliance.



Note This applies only to Cisco ISE Profiler and does not include NAC Profiler.

Step 3 Click the loglevel setting for the category of log:

- **OFF**: No log events are recorded for this category.
- **ERROR**: A log event is written to**/perfigo/control/tomcat/logs/nac_manager.log** only if the system encounters a severe error, such as:
  - CAM cannot connect to CAS
  - CAM and CAS cannot communicate
  - CAM cannot communicate with database
- **WARN**: Records only error and warning level messages for the given category.
- **INFO**: Provides more details than the **ERROR** and **WARN** log levels. For example, if a user logs in successfully an Info message is logged. This is the default level of logging for the system.
- **DEBUG**: Records all debug-level logs for the CAM.
- **TRACE**: This is the maximum amount of log information available to help troubleshoot issues with the CAM/CAS.

Step 4 Click **Update** to save the settings.



Note Cisco recommends using the **Debug** and **Trace** options only temporarily for very specific issues. Although the CAM records logging information and stores them in a series of ten 20MB files before discarding any old logs, the large amount of logging information can cause the CAM to run out of available log storage space in a relatively short amount of time.

For details on the Event Log, see Chapter 13, "Monitoring Event Logs."

Filtering Logs by CAS and/or Agent IP

Starting from Cisco NAC Appliance Release 4.9, you can filter the CAM Logs by CAS and/or Agent machine by specifying the IP Addresses. If the CAS in HA setup, then the service IP and eth0 addresses of both Active and Standby CAS should be entered for the filtering to happen properly.

Under **Filter by (Change log level for) CAS/Agent IP Address,** enter the following:

- **CAS IP Address:** Enter the IP Address of the specific CAS.
- **Agent IP Address:** Enter the IP Address of the specific client machine.

Note You can enter more than one IP Address by separating them with a comma. You can include the range of IP Addresses as well. For example, you can enter the IP Address as **10.10.10.10,10.10.10.15-20.**

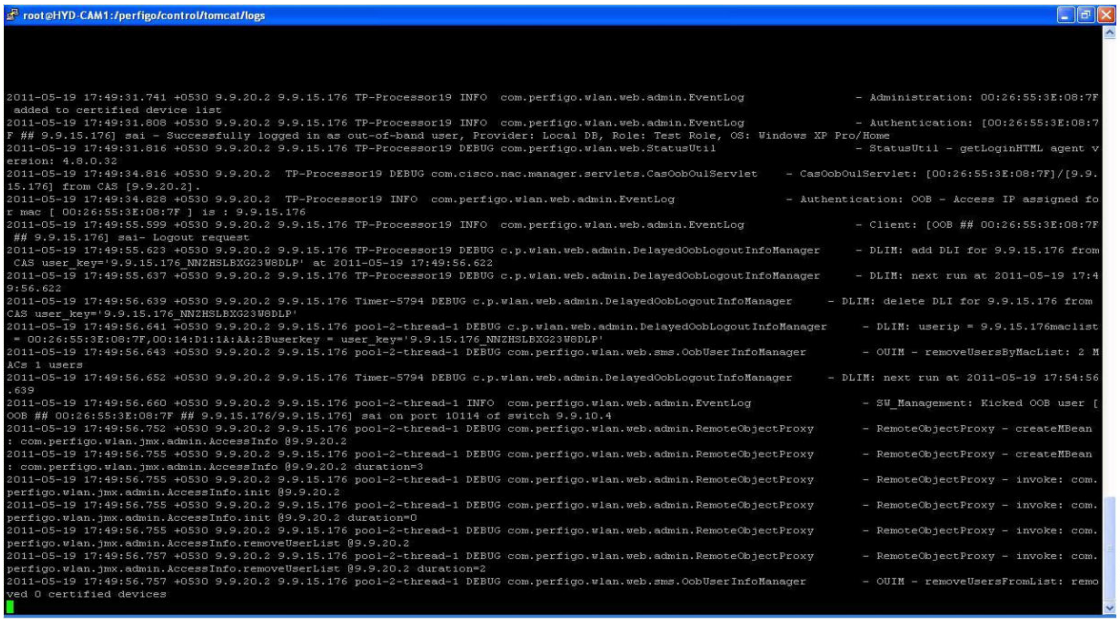
- **Log at Level:** Choose the log level.

Note To enable the Filter by CAS / Agent option, set the log levels of all the other categories to **OFF.**

Click **Update Filter** to save the settings. Download support logs to view information related to the specified CAS and Agent. To store all events to the **nac_manager.log** file, enable **Store all the events to log file** checkbox in the **Monitoring > Event Logs > Log Settings** page. This option is disabled by default. Refer to Limiting the Number of Logged Events, page 13-9.

Figure 14-31 shows an example of the Log file.

Figure 14-31 NAC Manager Logs


root@HYD-CAM1:/perfigo/control/tomcat/logs
2011-05-19 17:49:31.741 +0530 9.9.20.2 9.9.15.176 TP-Processor19 INFO com.perfigo.wlan.web.admin.EventLog - Administration: 00:26:55:3E:08:7F added to certified device list
2011-05-19 17:49:31.808 +0530 9.9.20.2 9.9.15.176 TP-Processor19 INFO com.perfigo.wlan.web.admin.EventLog - Authentication: [00:26:55:3E:08:7F ## 9.9.15.176] sai - Successfully logged in as out-of-band user, Provider: Local DB, Role: Test Role, OS: Windows XP Pro/Home
2011-05-19 17:49:31.816 +0530 9.9.20.2 9.9.15.176 TP-Processor19 DEBUG com.perfigo.wlan.web.StatusUtil - StatusUtil - getLoginHTML agent version: 4.8.0.32
2011-05-19 17:49:34.816 +0530 9.9.20.2 TP-Processor19 DEBUG com.cisco.nac.manager.servlets.CasOobOulServlet - CasOobOulServlet: [00:26:55:3E:08:7F]/[9.9.15.176] from CAS [9.9.20.2].
2011-05-19 17:49:34.828 +0530 9.9.20.2 TP-Processor19 INFO com.perfigo.wlan.web.admin.EventLog - Authentication: OOB - Access IP assigned for mac [00:26:55:3E:08:7F] is : 9.9.15.176
2011-05-19 17:49:55.599 +0530 9.9.20.2 9.9.15.176 TP-Processor19 INFO com.perfigo.wlan.web.admin.EventLog - Client: [OOB ## 00:26:55:3E:08:7F ## 9.9.15.176] sai- Logout request
2011-05-19 17:49:55.623 +0530 9.9.20.2 9.9.15.176 TP-Processor19 DEBUG c.p.wlan.web.admin.DelayedOobLogoutInfoManager - DLIM: add DLI for 9.9.15.176 from CAS user_key='9.9.15.176_NNZHSLBXG23W8DLP' at 2011-05-19 17:49:56.622
2011-05-19 17:49:55.637 +0530 9.9.20.2 9.9.15.176 TP-Processor19 DEBUG c.p.wlan.web.admin.DelayedOobLogoutInfoManager - DLIM: next run at 2011-05-19 17:49:56.622
2011-05-19 17:49:56.639 +0530 9.9.20.2 9.9.15.176 Timer-5794 DEBUG c.p.wlan.web.admin.DelayedOobLogoutInfoManager - DLIM: delete DLI for 9.9.15.176 from CAS user_key='9.9.15.176_NNZHSLBXG23W8DLP'
2011-05-19 17:49:56.641 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG c.p.wlan.web.admin.DelayedOobLogoutInfoManager - DLIM: userip = 9.9.15.176maclist = 00:26:55:3E:08:7F,00:14:D1:1A:AA:2Buserkey = user_key='9.9.15.176_NNZHSLBXG23W8DLP'
2011-05-19 17:49:56.643 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.sms.OobUserInfoManager - OUIM - removeUsersByMacList: 2 MACs 1 users
2011-05-19 17:49:56.652 +0530 9.9.20.2 9.9.15.176 Timer-5794 DEBUG c.p.wlan.web.admin.DelayedOobLogoutInfoManager - DLIM: next run at 2011-05-19 17:54:56.639
2011-05-19 17:49:56.660 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 INFO com.perfigo.wlan.web.admin.EventLog - SU_Management: Kicked OOB user [OOB ## 00:26:55:3E:08:7F ## 9.9.15.176/9.9.15.176] sai on port 10114 of switch 9.9.10.4
2011-05-19 17:49:56.752 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.admin.RemoteObjectProxy - RemoteObjectProxy - createMBean : com.perfigo.wlan.jmx.admin.AccessInfo @9.9.20.2
2011-05-19 17:49:56.755 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.admin.RemoteObjectProxy - RemoteObjectProxy - createMBean : com.perfigo.wlan.jmx.admin.AccessInfo @9.9.20.2 duration=3
2011-05-19 17:49:56.755 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.admin.RemoteObjectProxy - RemoteObjectProxy - invoke: com.perfigo.wlan.jmx.admin.AccessInfo.init @9.9.20.2
2011-05-19 17:49:56.755 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.admin.RemoteObjectProxy - RemoteObjectProxy - invoke: com.perfigo.wlan.jmx.admin.AccessInfo.init @9.9.20.2 duration=0
2011-05-19 17:49:56.755 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.admin.RemoteObjectProxy - RemoteObjectProxy - invoke: com.perfigo.wlan.jmx.admin.AccessInfo.removeUserList @9.9.20.2
2011-05-19 17:49:56.757 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.admin.RemoteObjectProxy - RemoteObjectProxy - invoke: com.perfigo.wlan.jmx.admin.AccessInfo.removeUserList @9.9.20.2 duration=2
2011-05-19 17:49:56.757 +0530 9.9.20.2 9.9.15.176 pool-2-thread-1 DEBUG com.perfigo.wlan.web.sms.OobUserInfoManager - OUIM - removeUsersFromList: removed 0 certified devices
246936

The CAM log statements are stamped by Agent and CAS IP address. The CAS log statements are stamped by Agent IP address.

Agent Logs

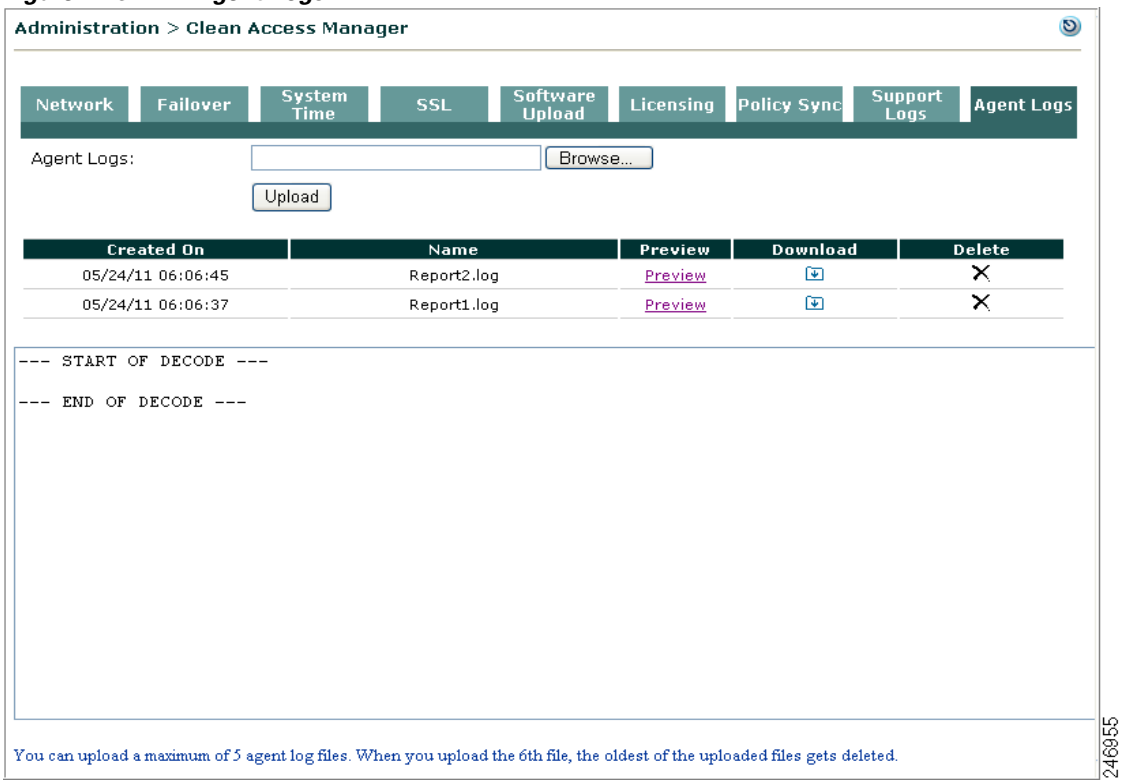
The **Agent Logs** page is available starting from Cisco NAC Appliance 4.9 and can be used to decrypt and upload the Agent Logs to the CAM. These Agent Logs are bundled with the CAM Support Logs into one tar file that can be sent to TAC to be included in the support case. Refer to Create Agent Log Files Using the Cisco Log Packager, page 11-6 for saving the Agent log files to your local machine.

Step 1 Go to **Administration > CCA Manager > Agent Logs**.

Step 2 Click the **Browse** button and navigate to the directory on your local machine where the Agent Logs file resides, select the file, and click **Upload**.

The uploaded files are listed in the **Agent Logs** page as shown in Figure 14-32.

Figure 14-32 Agent Logs



- You can click the **Preview** link next to the Agent Log file to view the contents. The contents of the file are displayed at the bottom of the page.
- Click the **Download** icon next to the file name to download the log file to your local system.

- Click the **Delete** icon next to the file name to remove the log file.

Note You can upload a maximum of five Agent Logs files to the CAM. When you upload the sixth file, the first file is automatically removed.

Admin Users

This section describes how to add multiple administrator users in the **Administration > Admin Users** module of the CAM web admin console.

Under **Administration > Admin Users** there are three tabs: **Admin Groups**, **Admin Users**, and **Access Restrictions**.

You can create new admin users and associate them to pre-existing default admin groups, or you can create your own custom admin groups. In either case, the access permissions defined for the admin group are applied to admin users when you add those users to the group.

You can also choose to authenticate admin user credentials entered in both the CAM and CAS via an external Kerberos, LDAP, or RADIUS authentication server (configured using the instructions in Adding an Authentication Provider, page 7-4), or using the local CAM database. See Add an Admin User, page 14-51 for details.

Admin Groups

There are three default (uneditable) admin groups in the system, and one predefined custom group ("Help Desk") that you can edit. In addition, you can also create any number of your own custom admin groups under **Administration > Admin Users > Admin Groups > New**.

The four default admin group types are:

1. Hidden
2. Read-Only
3. Add-Edit
4. Full-Control (has delete permissions)

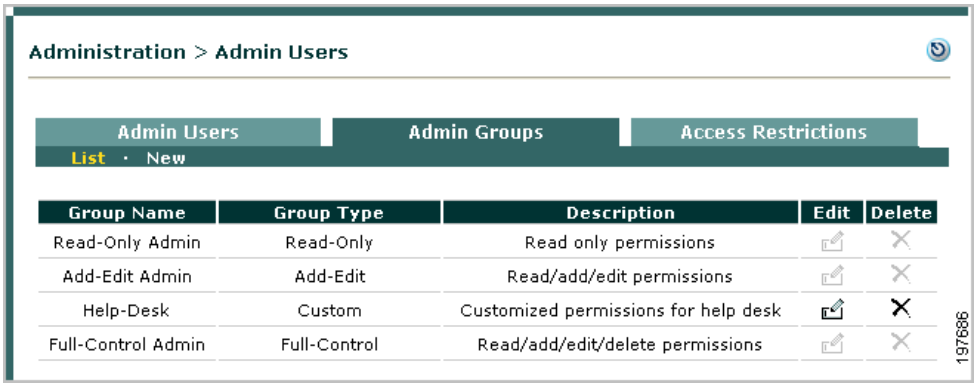
The three default admin group types cannot be removed or edited. You can add users to one of the three pre-defined groups, or you can configure a new Custom group to create specialized permissions. When creating custom admin permissions, create and set access permissions for the custom admin group first, then add users to that group to set their permissions.

Add/Edit a Custom Admin Group

To create a new admin group:

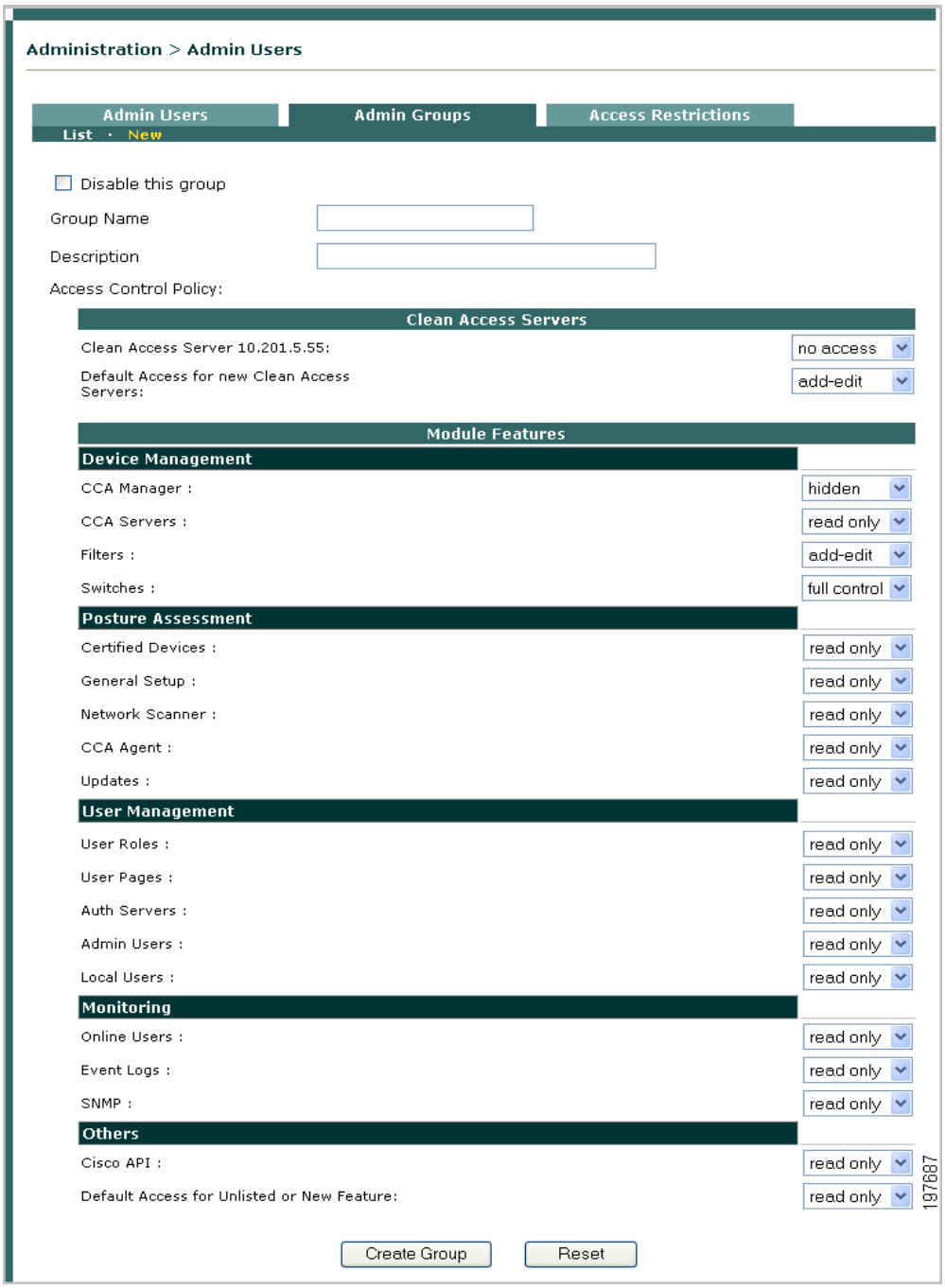
Step 1 Go to **Administration > Admin Users > Admin Groups**.

Figure 14-33 Admin Groups



Step 2 Click the **New** link to bring up the new Admin Group configuration form.

Figure 14-34 New Admin Group



Step 3 Click the **Disable this group** checkbox if you want to initially create but not yet activate this new administrator group, or if you want to disable an existing administrator group.

Step 4 Enter a **Group Name** for the custom admin group.

Step 5 Enter an optional **Description** for the group.

Step 6 Set the access options next to each individual Clean Access Server as **no access**, **view only**, **add-edit**, or **local admin**. This allows you to restrict access to the individual Clean Access Server for a specified administrator group, enable an administrator group to view permissions on the individual Clean Access Server, and even tailor access to provide an administrator group full control over one or more Clean Access Servers (including delete/reboot capabilities).

Note When a Clean Access Server option is set to **no access**, the members of the administrator group can still see the specified server in the **Device Management > CCA servers > List of Servers** page, but they cannot manage, disconnect, reboot or delete the server.

Step 7 Select group access privileges of **hidden**, **read only**, **add-edit**, or **full control** for each individual module or submodule. This allows you to limit the Clean Access Server modules and submodules available to a specified administrator group and tailor administrative control over modules and/or submodules for the specified administrator group.

Note When a submodule option is set to **hidden**, the members of the administrator group can still see the given submodule in the left-hand web console pane, but the text is "greyed out" and they cannot access that submodule.

Step 8 Click **Create Group** to add the group to the Admin Groups list.

You can edit the group later by clicking the **Edit** icon next to the group in the list. To delete the group click the **Delete** icon next to the group. Users in an admin group are not removed when the group is deleted, but are assigned to the default **Read-Only Admin** group.

Note If an administrator changes the permissions of a particular admin group by editing the admin group, the administrator must remove all admin users belonging to that group since the new permissions will only be effective from the next login.

Admin Users

Note The default **admin** user is in the default **Full-Control Admin** group and is a special system user with full control privileges that can never be removed from the Clean Access Manager. For example, a Full-Control user can log in and delete his/her own account, but one cannot log in as user **admin** and delete the **admin** account.

Admin users are classified according to Admin Group. The following general rules apply:

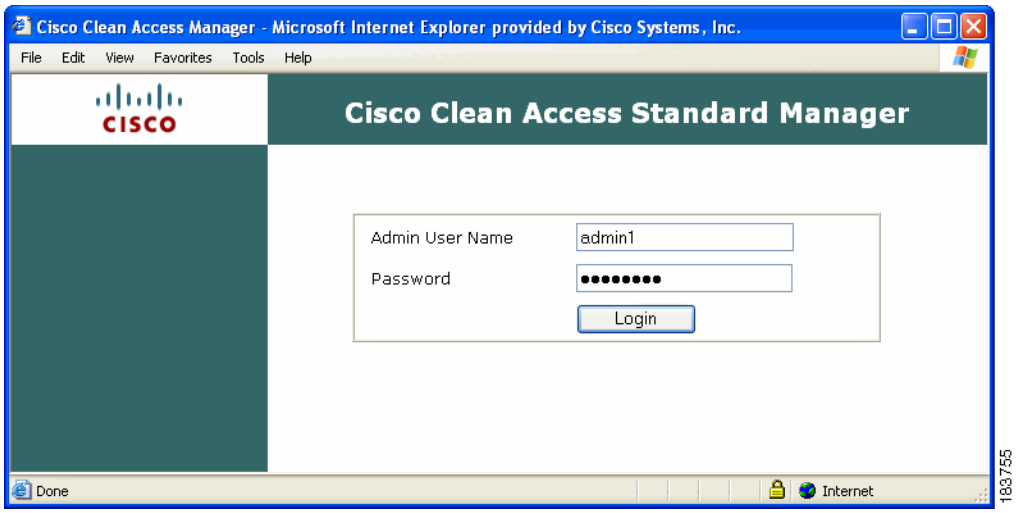
- All admin users can access the **Administration > Admin Users** module and change their own passwords.
- Features that are not available to a level of admin user are simply disabled in the web admin console.
- Read-Only users can only view users, devices, and features in the web admin console.
- Add-Edit users can add and edit but not remove local users, devices, or features in the web admin console. Add-Edit admin users cannot create other admin users.

- Full-Control users can add, edit, and delete all applicable aspects of the web admin console.
- Only Full-Control admin users can add, edit, or remove other admin users or groups.
- Custom group users (part of the "Help-Desk" admin group type, for example) can be configured to have a combination of access privileges, as described in Add/Edit a Custom Admin Group, page 14-47.

Login/Logout an Admin User

As admin users are session-based, admin users should log out using the Logout icon in the top-right corner of every page of the web admin console. The administrator login page will appear:

Figure 14-35 Admin Login



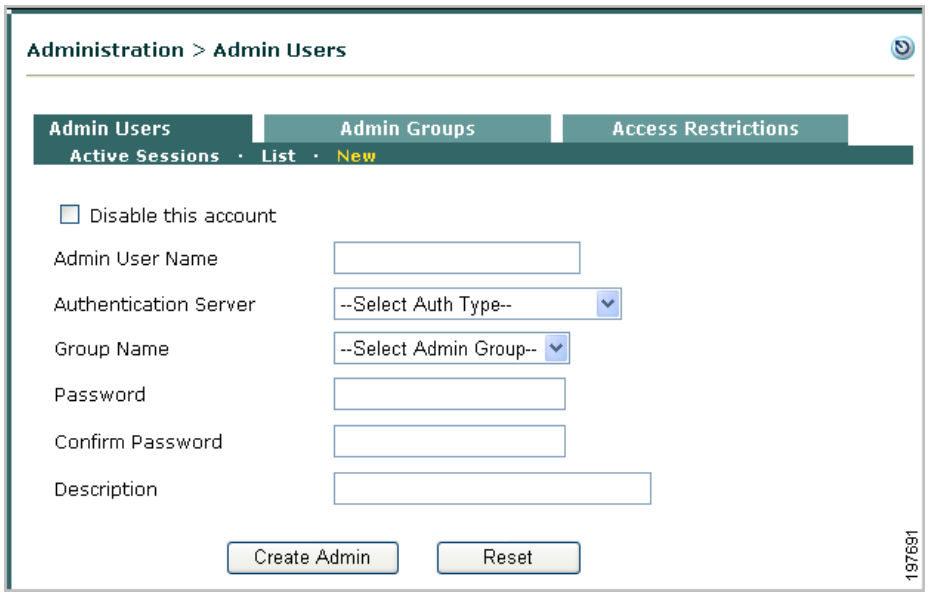
Additionally, you can use the logout button to log out as one type of admin user and relogin on as another.

Add an Admin User

To add a new administrator user:

Step 1 Go to **Administration > Admin Users > New**.

Figure 14-36 New Admin User



Step 2 Click the **Disable this account** checkbox if you want to initially create but not yet activate this new administrator user profile, or if you want to disable an existing administrator user.

Step 3 Enter an **Admin User Name**.

Step 4 For the **Authentication Server** dropdown menu, specify the method by which the CAM authenticates the administrator user login credentials entered in the CAM and/or CAS:

- Choose **Built-in Admin Authentication** to verify administrator user credentials against the information stored locally in the CAM database.
- Choose the Provider Name of a configured Kerberos, LDAP, or RADIUS authentication server to authenticate the admin user against an external authentication server. For admin users, only Kerberos, LDAP and RADIUS authentication servers are listed in the **Authentication Server** dropdown. See Adding an Authentication Provider, page 7-4 for details.

Step 5 Select an admin group type from the **Group Name** dropdown list. Default groups are Read-Only, Add-Edit, and Full-Control. To add a user to a custom-access permissions group, add the group first as described in Add/Edit a Custom Admin Group, page 14-47.

Step 6 Enter a password in the **Password** and **Confirm Password** fields.

Step 7 Enter an optional **Description**.

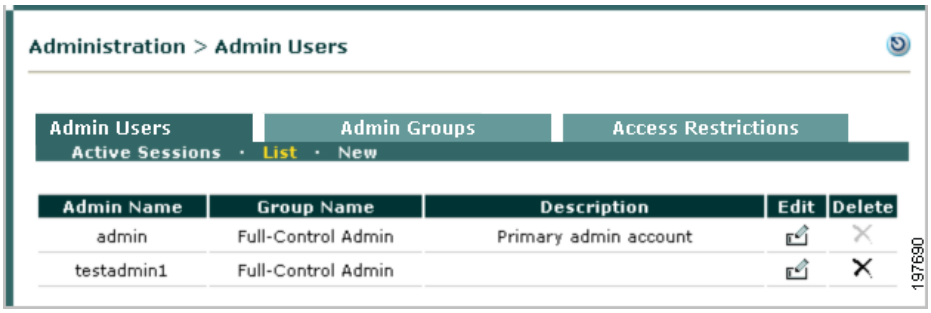
Step 8 Click **Create Admin**. The new user appears under the **Admin Users > List**.

Edit an Admin User

To edit an existing admin user:

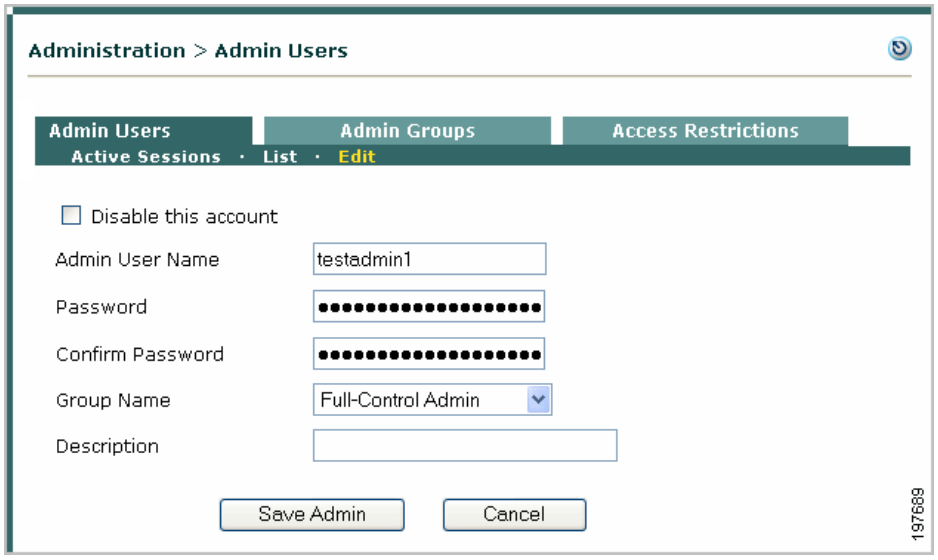
Step 1 Go to **Administration > Admin Users > List**.

Figure 14-37 Admin Users List



Step 2 Click the **Edit** icon next to the admin user.

Figure 14-38 Edit Admin User



Step 3 Change the **Password** and **Confirm Password** fields, or other desired fields.

Step 4 Click **Save Admin**.

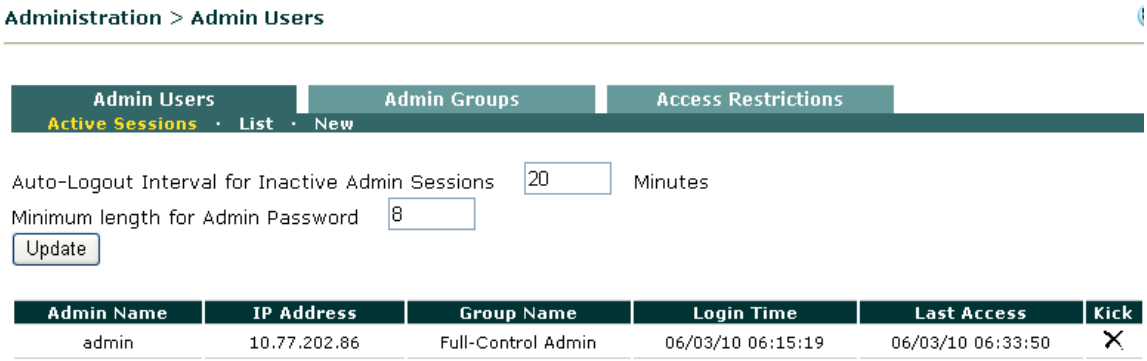
Note You can edit all properties of the system **admin** user, except its group type.

Active Admin User Sessions

You can view which admin users are using the Clean Access Manager web admin console from **Administration > Admin Users > Admin Users > Active Sessions**. The **Active Sessions** list shows all admin users that are currently active. Admin users are session-based. Each browser that an admin user opens to connect to the Clean Access Manager webserver creates an entry for the user in the **Active Sessions** list.

If an admin user opens a browser, closes it, then opens a new browser, two entries will remain for a period of time on the **Active Session** list. The Last Access time does not change for the ended session, and eventually the entry will be removed by the Auto-logout feature.

Figure 14-39 Admin User Active Sessions



The **Active Sessions** page includes the following elements:

- **Admin Name**—The admin user name.
- **IP Address**—The IP address of the admin user's machine.
- **Group Name**—The access privilege group of the admin user.
- **Login Time**—The start of the admin user session.
- **Last Access**—The last time the admin user clicked a link anywhere in the web admin console. Each click resets the last access time.
- **"Auto-Logout Interval for Inactive Admins"**—This value is compared against the Login Time and Last Access time for an active admin user session. If the difference between the current time and last access time is greater than the auto-logout interval configured, the user is logged out. This value must be in the range of 1 to 120 minutes, with an interval of 20 minutes set by default.
- **"Minimum length for Admin Password"**—Enter a value here to set minimum password length for the Admin Password.
- **Kick**—Clicking this button logs out an active admin user and removes the session from the active session list.

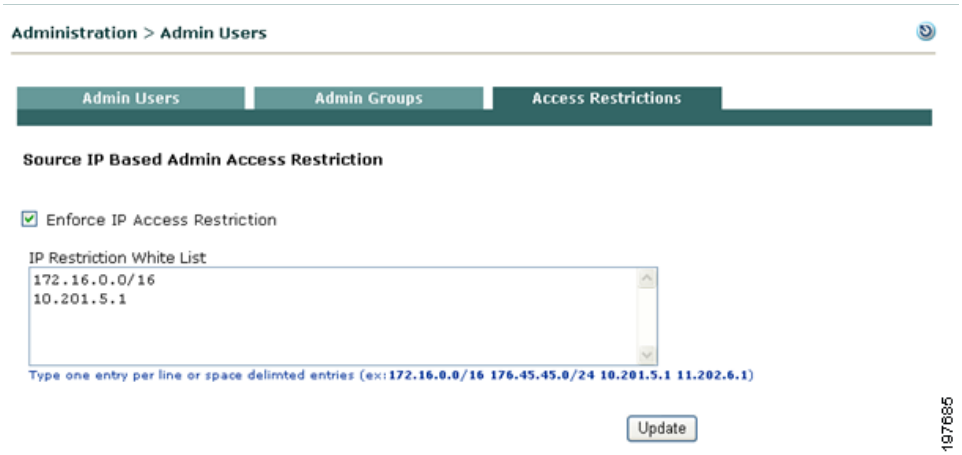
Administrator User Access Restrictions

The admin user can configure a set of IP addresses of the CAM and CAS web console/SSH that can be blocked. The access is restricted to the list of IP addresses provided by the administrator.

Use the following procedure to enable the access restriction.

Step 1 Go to **Administration > Admin Users > Access Restrictions**.

Figure 14-40 Administrator User Access Restrictions



Step 2 Check the **Enforce IP Access Restriction** checkbox.

Step 3 In the **IP Restriction White List** box, enter the IP Addresses to be allowed by the CAM and CAS. Type one address per line.

Step 4 Click **Update**.

Step 5 Both the CAM and CAS are enabled with the list of IP Addresses provided.

Note The access list is applied only to the CAS that is already added to the CAM.

Note If you uncheck the **Enforce IP Access Restriction** checkbox, the IP addresses provided in the list become inactive. The access restriction is not enforced.

Caution If you click **Update** when the **IP Restriction White List** field is empty, the CAM/CAS are made inaccessible via web console or SSH. If this happens, you can use the following procedure to unlock CAM/CAS access again.

The following procedure provides instructions on how to unlock the CAM web console. You need to use the Serial Console or keyboard/monitor to access the CAM.

Step 1 Delete the contents of the **/perfigo/control/apache/conf/sslacc.conf** file in CAM.

Step 2 Run the command **/perfigo/control/bin/startapache_g** in CAM.

Step 3 This will unlock CAM web console.

Step 4 Login to the CAM web console, edit the access restriction list, and click **Update**.

Note Once you complete the above steps, both the CAM and CAS are accessible. If you are using HA pairs, you must execute the steps for both the CAMs.

Manage System Passwords

Note For new installations of Cisco NAC Appliance, the root administrator user password must conform to the strong password guidelines outlined below. Existing root administrator user passwords are preserved during upgrade.

It is important to provide secure passwords for the user accounts in Cisco NAC Appliance system, and to change them from time to time to maintain system security. Cisco NAC Appliance prompts you to specify the following administrative user account passwords:

1. Clean Access Manager installation machine **`root`** user
2. Clean Access Server installation machine **`root`** user
3. Clean Access Server web console **`admin`** user
4. Clean Access Manager web console **`admin`** user

Passwords are initially set at installation time. To change these passwords at a later time, access the CAM or CAS machine by SSH, logging in as the user whose password you want to change. Use the Linux **`passwd`** command to change the user's password.

In all cases, Cisco recommends using strong passwords to maximize network security, but only the root administrator passwords on the CAM and CAS are *required* to conform to the strong password criteria, that is, passwords containing at least eight characters that feature at least two characters from each of the following four categories:

- Lower-case letters
- Upper-case letters
- Numbers (digits)
- Special characters (like !@#$%^&*~)

For example, the password **`10-9=One`** would not satisfy the requirements because it does not feature two characters from each category, but **`1o-9=OnE`** is a valid password.

Note If the first character of a password is an upper-case letter, that character is not counted toward the minimum number of required upper-case letters (two) when determining whether or not the correct number of characters exists in the password.

If the last character of a password is a digit, that character is not counted toward the minimum number of required digits (two) when determining whether or not the correct number of characters exists in the password.

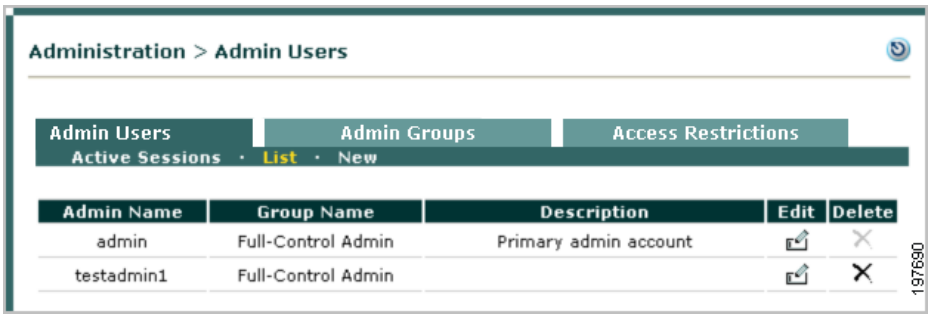
This section describes the following:

- Change the CAM Web Console Admin Password
- Change the CAS Web Console Admin User Password

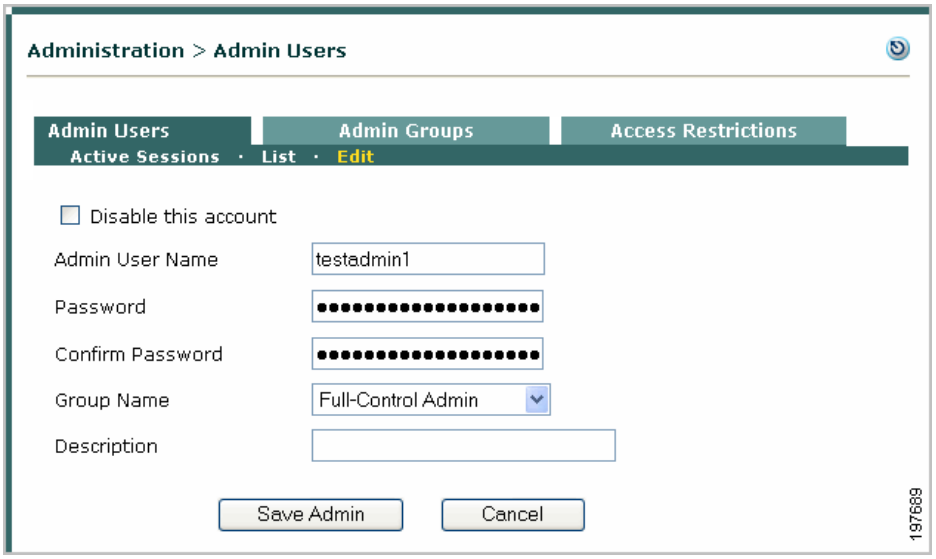
Change the CAM Web Console Admin Password

To change the Clean Access Manager web console admin user password, use the following procedure.

Step 1 Go to **Administration > Admin Users > List**.



Step 2 Click the **Edit** icon for user **admin**.



Step 3 Type the new password in the **Password** field.

Step 4 Type the password again in the **Confirm Password** field.

Step 5 Click the **Save Admin** button. The new password is now in effect.

Change the CAS Web Console Admin User Password

Most configuration tasks are performed in the CAM web admin console. However, the CAS direct access web console is used to perform several tasks specific to a local CAS configuration, such as configuring High-Availability mode. Use the following instructions to change the CAS web console admin password:

Step 1 Open the Clean Access Server admin console by navigating to the following address in a browser:

`https://<CAS_IP>/admin`
where **`<CAS_IP>`** is the trusted interface IP address of the CAS. For example,
`https://172.16.1.2/admin`

Step 2 Log in with the **`admin`** user name and password.

Step 3 Click the **Admin Password** link from the left side menu.

Step 4 In the **Old Password** field, type the current password.

Step 5 Type the new password in the **New Password** and the **Confirm Password** fields.

Step 6 Click **Update**.

Backing Up the CAM Database

You can create a manual backup snapshot of the CAM database to backup the CAM/CAS configuration for the current release. When you create the snapshot, it is saved on the CAM, but you can also download it to another machine for safekeeping. Only the CAM snapshot needs to be backed up. The CAM snapshot contains all database configuration data for the Clean Access Manager, and configuration information for all Clean Access Servers added to the CAM's domain. The snapshot is a standard postgres data dump.

The Clean Access Manager uses a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to restore database snapshots on the CAM when you need them. (You cannot upload a CAM database snapshot that was created when the system was configured with a different master secret password.)

Note Product licenses are stored in the database and are therefore included in the backup snapshot.

Once a CAS is added to the CAM, the CAS gets its configuration information from the CAM every time it contacts the CAM, including after a snapshot configuration is downloaded to the CAM.

If you replace the underlying machine for a CAS that is already added to the CAM, you will need to execute the **`service perfigo config`** utility to configure the new machine with the CAS IP address and certificate configuration. Thereafter, the CAM pushes all the other configuration information to the CAS.

The Agent is always included as part of the CAM database snapshot. The Agent is always stored in the CAM database when:

- The Agent update is received from web updates
- The Agent is manually uploaded to the CAM

However, when the CAM is newly installed from CD or upgraded to the latest release, the Agents are not backed up to the CAM database. In this case, the CAM software contains the new Agent software but this is not uploaded to the CAM database. Agent backups only start when a new Agent is uploaded to the system either manually or by web updates.

Note You can only restore a CAM snapshot that has the same version as the CAM (e.g. release 4.9 snapshot to release 4.9 CAM).

Note For further details on database logs, refer to Cisco NAC Appliance Log Files, page 13-11.

This section describes the following:

- Automated Daily Database Backups
- Manual Backups from Web Console
- Restoring a CAM Snapshot—Standalone CAM
- Restoring a CAM Snapshot—HA-CAM or HA-CAS
- Backing Up and Restoring CAM/CAS Authorization Settings
- Backing Up and Restoring CAM/CAS Authorization Settings
- Database Recovery Tool

Automated Daily Database Backups

Cisco NAC Appliance automatically creates daily snapshots of the Clean Access Manager database and preserves the most recent from the last 30 days. It also automatically creates snapshots before and after software upgrades, and before and after failover events. For upgrades and failovers, only the last 5 backup snapshots are kept. See Database Recovery Tool, page 14-64 for additional details.

Manual Backups from Web Console

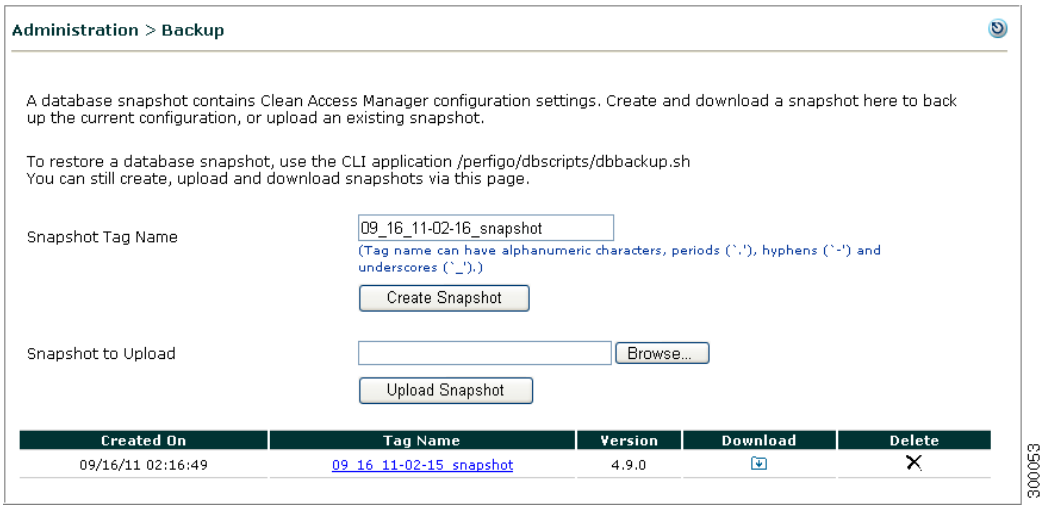
Cisco recommends creating a backup of the CAM before making major changes to its configuration. Backing up the configuration from time to time also ensures a recent backup of a known-good configuration profile, in case of a malfunction due to incorrect settings. Besides protecting against configuration data loss, snapshots provide an easy way to duplicate a configuration among several CAMs.

Note Manually-created snapshots stay on the CAM until they are manually removed.

Step 1 In the **Administration > Backup** page, type a name for the snapshot in the **Database Snapshot Tag Name** field. The field automatically populates with a filename that incorporates the current date and time (e.g `MM_DD_YY-hh-mm_snapshot`). You can either accept the default name or type another.

Step 2 Click **Create Snapshot**. The Clean Access Manager generates a snapshot file, which is added to the snapshot list. The **Version** column automatically lists the CAM software version for the snapshot.

Figure 14-41 Backup Snapshot


Administration > Backup
A database snapshot contains Clean Access Manager configuration settings. Create and download a snapshot here to back up the current configuration, or upload an existing snapshot.
To restore a database snapshot, use the CLI application /perfigo/dbscripts/dbbackup.sh
You can still create, upload and download snapshots via this page.
Snapshot Tag Name
09_16_11-02-16_snapshot
(Tag name can have alphanumeric characters, periods (`.'), hyphens (`-') and underscores (`_').)
Create Snapshot
Snapshot to Upload
Browse...
Upload Snapshot
Created On
Tag Name
Version
Download
Delete
09/16/11 02:16:49
09_16_11-02-15_snapshot
4.9.0
300053

Note The file still physically resides on the Clean Access Manager machine. For archiving purposes, it can remain there. However, to back up a configuration for use in case of system failure, the snapshot should be downloaded to another computer.

Step 3 To download the snapshot to another computer, click either the **Download** icon or the **Tag Name** of the snapshot that you want to download.

Step 4 In the **File Download** dialog, **Save** the file to your local computer.

To remove the snapshot from the snapshot list, click the **Delete** icon.

Restoring a CAM Snapshot—Standalone CAM

Note You can only restore a CAM snapshot that has the same version as the CAM (e.g. release 4.9 snapshot to release 4.9 CAM) and, although you can use the CAM web console to upload the snapshot image you want to restore, you must perform the actual restoration step via the CAM CLI.

The Clean Access Manager uses a local master secret password to encrypt and protect important data, like other system passwords. Cisco recommends keeping very accurate records of assigned master secret passwords to ensure that you are able to restore database snapshots on the CAM when you need them. (You cannot upload a CAM database snapshot that was created when the system was configured with a different master secret password.) To restore a standalone Clean Access Manager to the configuration state of the snapshot:

Step 1 Go to **Administration > Backup**, ensure the snapshot image **Tag Name** appears in the table, and that the version of the snapshot is the same version currently running on the CAM.

Step 2 If you need to upload the snapshot image from an external machine first, click the **Browse** button next to the **Snapshot to Upload** field, find the file in the external directory structure, and click **Upload Snapshot**.

Step 3 Log into the CAM CLI console and shut down services on the CAM using the `service perfigo stop` command.

Step 4 Enter the `/perfigo/dbscripts/dbbackup.sh` command. The existing configuration is overridden by the configuration in the snapshot.

Warning **Entering the "./dbbackup.sh" command using "sh ./dbbackup.sh"syntax can cause the backup process to enter an endless loop, repeatedly asking you to verify the restoration process. Do not use the "sh ./dbbackup.sh"syntax.**

Step 5 Restart services on the CAM using the `service perfigo start` command.

Restoring a CAM Snapshot—HA-CAM or HA-CAS

Note The CAM snapshot contains all database configuration data for the Clean Access Manager and configuration information for all Clean Access Servers added to the CAM's domain.

If either of the HA-Primary and HA-Secondary CAMs and/or CASs in your HA deployment lose their configuration, you can retrieve the most recent snapshot (or create one for the existing configuration) from the remaining CAM and load it into your HA system to ensure consistent behavior from both the HA-Primary and HA-Secondary machines.

If *both* the HA-Primary and HA-Secondary CAMs and or CASs in your HA deployment lose their configuration, you can restore the system using the following guidelines. (For example, if a catastrophic event wipes out the image and database on both the HA-Primary and HA-Secondary machines or forces you to RMA both machines and install new appliances.)

Warning **Do not attempt to restore a snapshot on either the active or standby CAM if the standby machine is offline (down or still rebooting).**

Restore Both HA-Primary and HA-Secondary CAMs from Snapshot

To restore the HA-Primary and HA-Secondary CAMs in a failover deployment to the configuration state of the snapshot:

Step 1 Install and initially configure the HA-Primary CAM and HA-Secondary CAM so that they feature the same attributes as before your HA deployment went down as described in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Step 2 Apply your CAM user license(s) to both the HA-Primary and HA-Secondary CAMs.

Step 3 Reconfigure the HA-Primary and HA-Secondary CAMs as an HA pair as described in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Step 4 Shut down the HA-Secondary CAM to prevent it from automatically assuming the "active" role during database restoration.

Step 5 Navigate to the **Administration > Backup** web console page on the HA-Primary CAM, click the **Browse** button next to the **Snapshot to Upload** field, find the file in the external directory structure, and click **Upload Snapshot**.

Step 6 Log into the HA-Primary CAM CLI console and shut down services on the CAM using the `service perfigo stop` command.

Step 7 Enter the `/perfigo/dbscripts/dbbackup.sh` command. The existing configuration is overridden by the configuration in the snapshot.

Warning **Entering the "./dbbackup.sh" command using "sh ./dbbackup.sh"syntax can cause the backup process to enter an endless loop, repeatedly asking you to verify the restoration process. Do not use the "sh ./dbbackup.sh"syntax.**

Step 8 Restart services on the HA-Primary CAM using the `service perfigo start` command.

Step 9 To complete the snapshot restoration, bring up the HA-Secondary CAM and wait approximately 5 minutes for the HA-Secondary CAM to automatically "sync up" with the HA-Primary.

Step 10 Reboot the HA-Primary CAM. Once the CAM has restarted and you can log in via the web console, reboot the HA-Secondary CAM.

Restore Both HA-Primary and HA-Secondary CASs from Snapshot

To restore the HA-Primary and HA-Secondary CASs in a failover deployment to the configuration state of the snapshot:

1. Install and initially configure the HA-Primary CAS and HA-Secondary CAS so that they feature the same attributes as before your HA deployment went down as described in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.
2. Reconfigure both the HA-Primary and HA-Secondary CASs as an HA pair as described in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Warning **Ensure you follow the instructions in the "Configuring High Availability (HA)" chapter in the order they are presented to successfully re-establish your CAS HA connection.**

3. Simulate failover events between the HA-Primary and HA-Secondary CASs by shutting down/disconnecting the HA-Primary CAS to allow the HA-Secondary CAS to assume access control functions. Once the standby CAS assumes the active role, simulate the same failover for the HA-Secondary CAS (the new active CAS) when the HA-Primary (standby) comes back "online."

   Performing these failover simulations on both the HA-Primary and HA-Secondary CASs ensures that each one gets the current database information from the CAM.

Backing Up and Restoring CAM/CAS Authorization Settings

As an added security measure, Authorization and certificate trust store settings are not backed up with other elements of the CAM/CAS configuration. Therefore, when backing up your CAM/CAS configuration, you must back up Authorization and certificate trust store files separately from the standard database backup/snapshot.

For high-availability pairs, Authorization settings are not automatically passed from the HA-Primary CAM/CAS to the HA-Secondary when deployed as a high-availability pair. You can also use the following procedure to populate the Authorization settings on an HA-Secondary CAM/CAS to ensure both appliances in the HA-pair share exactly the same Authorization and certificate trust store settings and list of Authorized Clean Access Servers (or Clean Access Managers if backing up an HA-Primary Clean Access Server).

Note If you have a large CAS deployment managed from a single CAM, this procedure can save considerable time when configuring the secondary CAM.

Table 14-2 lists the files typically found in the **/root/.perfigo/** directory (depending on your particular configuration).

Table 14-2 Authorization Backup Files

File Name	Description
auth_nac_en.txt	If this file is present in the CAM/CAS's **/root/.perfigo/** directory, the CAM/CAS has enabled the Authorization feature.
auth_nac.txt	This file contains the actual Clean Access Manager or Clean Access Server Authorization entries that populate the Authorized CCA Servers/Authorized CCA Managers lists on the CAM **Device Management > CCA Servers > Authorization** web console page or CAS **Device Management > Authorization** web console page.
auth_warn_nac_en.txt	If this file is present in the CAM/CAS's **/root/.perfigo/** directory, the CAM/CAS has enabled the **Test CCA Server Authentication** option and is logging Authorization operations as SSL Certificate events.
caCerts	This file contains the collection of end entity certificates on the CAM/CAS.

To back up CAM/CAS Authorization and certificate trust store settings and upload them to a redundant or HA-Secondary CAM/CAS:

Step 1 Telnet or SSH to the command line interface of the primary CAM/CAS, navigate to the **/root/.perfigo/** directory, and view the contents of the **/root/.perfigo/** directory:

```
[root@cam1]# cd /root/
[root@cam1]# cd .perfigo/
[root@cam1]# ls -l
-rw-r--r--  1 root root    0 Jul 21 11:09 auth_nac_en.txt
-rw-r--r--  1 root root   80 Jul 21 11:09 auth_nac.txt
-rw-r--r--  1 root root   16 Jul 21 11:09 auth_warn_nac_en.txt
-rw-r--r--  1 root root 1346 Jul 20 21:49 caCerts
```

Step 2 Create the tar file to upload. You will need to specify a file name (for example, "authorization.tar.gz").

```
[root@cam1]# tar cvzf authorization.tar.gz *
auth_nac_en.txt
auth_nac.txt
auth_warn_nac_en.txt
caCerts
```

Step 3 Upload the new tar file to the destination CAM/CAS for backup or to populate an HA-Standby CAM/CAS.

```
[root@cam1]# scp authorization.tar.gz root@<IP address>
root@<IP address>'s password:
authorization.tar.gz                                  100% 1107     1.1KB/s   00:00
```

Step 4 Telnet or SSH to the command line interface of the secondary CAM/CAS, navigate to the **/root/.perfigo/** directory, and extract the contents of the uploaded tar file.

```
[root@cam2]# cd /root/
[root@cam2]# cd .perfigo/
[root@cam2]# tar xvzf authorization.tar.gz
auth_nac_en.txt
auth_nac.txt
auth_warn_nac_en.txt
caCerts
```

Step 5 Verify that the files have been uploaded and extracted correctly.

```
[root@cam2]# ls -l
-rw-r--r--  1 root root    0 Jul 21 11:09 auth_nac_en.txt
-rw-r--r--  1 root root   80 Jul 21 11:09 auth_nac.txt
-rw-r--r--  1 root root   16 Jul 21 11:09 auth_warn_nac_en.txt
-rw-r--r--  1 root root 1346 Jul 20 21:49 caCerts
```

Step 6 Stop and Restart the secondary CAM/CAS to apply the duplicate settings.

```
[root@cam2]# service perfigo stop
Stopping High-Availability services:
[  OK  ]
[root@cam2]# service perfigo start
Starting High-Availability services:
[  OK  ]
Please wait while bringing up service IP.
Heartbeat service is running.
Service IP is up on the peer node.
Stopping postgresql service: [  OK  ]
Starting postgresql service: [  OK  ]
CREATE DATABASE
DROP DATABASE
CREATE DATABASE
DROP DATABASE
Database synced
[root@cam2]#
```

Note This example addresses a CAM HA-pair, but the same functions and process apply to a CAS HA-pair.

For more information on CAM and CAS HA-pairs, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Database Recovery Tool

The Database Recovery tool is a command line utility that can be used to restore the database from the following types of backup snapshots:

- Automated daily backups (the most recent 30 copies)
- Backups made before and after software upgrades

- Backups made before and after failover events
- Manual snapshots created by the administrator via the web console

Although the web console already allows you to manually create and upload snapshots (via **Administration > Backup**), the CLI tool presents additional detail. The tool provides a menu that lists the snapshots from which to restore, and the uncompressed size and table count. Note that a file which is corrupt or not in the proper format (e.g. not .tar.gz) will show a remediation warning instead of an uncompressed size and a table count.

Caution The CAM must be stopped before you can run this utility and must be rebooted after the utility is run.

To run the command utility:

1. Access your Clean Access Manager by SSH.
2. Login as user `root` with the root password.
3. CD to the directory of the database recovery tool: `cd /perfigo/dbscripts`.
4. Run `service perfigo stop` to stop the Clean Access Manager.
5. Run `./dbbackup.sh` to start the tool.

Warning **Entering the "./dbbackup.sh" command using "sh ./dbbackup.sh"syntax can cause the backup process to enter an endless loop, repeatedly asking you to verify the restoration process. Do not use the "sh ./dbbackup.sh"syntax.**

6. Follow the prompts to perform database restore.
7. Run `reboot` to reboot the Clean Access Manager after running the utility.

Note For general information on CLI commands, see the "CAM CLI Commands" section in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

API Support

Cisco NAC Appliance provides a utility script called **cisco_api.jsp** that allows you to perform certain operations using HTTPS POST. The Cisco NAC Appliance API for your Clean Access Manager is accessed from a web browser as follows: **https://<ccam-ip-or-name>/admin/cisco_api.jsp.**

For usage and authentication requirements, guest access support, and operations summary information, see Appendix B, "API Support".



Error and Event Log Messages

Client Error Messages

Login Failed

```
Clean Access Server is not properly configured, please report to your administrator.
```

A login page must be added and present in the system in order for both web login and Agent users to authenticate. If a default login page is not present, Agent users will see this error dialog when attempting login. See also Add Default Login Page, page 5-3.

```
Clean Access Server could not establish a secure connection to the Clean Access Manager at
<IP_address>
```

This error message to clients attempting login commonly indicates one of the following issues:

- The time difference between the CAM and CAS is greater than 5 minutes.
- Invalid IP address
- Invalid domain name
- CAM is unreachable

See also Troubleshooting Certificate Issues, page 14-21.

Network Error

```
The request has timed out. [12002]
```

This error indicates a communication issue between the Agent and the CAS. The Agent pops up initially indicating that the Agent is able to reach the CAS and vice versa. However, at some point the communication is lost resulting in the error message. This error can reflect a timing issue after the VLAN has been changed for the user machine in OOB deployments. Increasing the **VLAN Change Delay** (under **OOB Management > Profiles > SNMP Receiver > Advanced Settings**) from the 2 second default to 3 or 4 seconds may resolve the issue.

Users Cannot Log In During CAS Fallback Recovery

```
Failed to add user to the list
```

During CAS fallback recovery (where the CAS is reconnecting to the CAM), a login dialog appears to users accessing the Cisco NAC Appliance network via the CAS, but they are unable to authenticate and login for approximately 2 minutes. (Until CAS fallback recovery completes, users see a "Failed to add user to the list" error message when attempting to log in.)

For more information on CAS Fallback design and implementation, see the "CAS Fallback Policy" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

CAM Event Log Messages

Table A-1 describes Clean Access Manager event log messages. You can view the even log in the Clean Access Manager admin console from **Monitoring > Event Logs**.

Table A-1 Event Log Messages (Sheet 1 of 4)

Message	Explanation	Severity
<MAC address> added to AP MAC list	The access point is successfully added to the access point list.	Normal configuration log
<MAC address> could not be added to the AP MAC list	Adding access point to a passthrough list failed; the Clean Access Server might not be connected.	Error occurred when trying to automatically add to passthrough list
<MAC address> removed from the MAC list	Access point removed from the list.	Normal configuration log
<MAC address> could not be removed from the AP MAC list	Removing the access point from the passthrough list failed; the Clean Access Server might not be connected.	Error occurred when trying to remove from a passthrough list
<Authentication Server Name> added to authentication server list	Authentication server is added to the list.	Normal configuration log
<Authentication Server Name> is already configured in authentication server list	Authentication server being added is already on the list.	Normal configuration log
Provider name <Authentication Server Name> is already been used by different authentication server	Authentication server name already in use; updating authentication server failed.	Error on authentication server update
<Authentication Server Name> updated to authentication server list	Authentication server updated successfully.	Normal configuration log
<Authentication Server Name> is not a valid authentication server	Authentication server update failed; not a valid authentication server.	Error on authentication server update
<Authentication Server Name> removed from the authentication server list	Authentication server removed successfully.	Normal configuration log
<User name, MAC, IP> - Logout request	IPSec Client user logout request.	Normal configuration log
<User name, MAC, IP> - Logout attempt failed;	User logout failed; Clean Access Server is not connected.	Error

Table A-1 Event Log Messages (Sheet 2 of 4)

Message	Explanation	Severity
Invalid user credentials, <User name, MAC, IP>	Username and password invalid.	Error
Invalid authentication provider, <Provider Name> <User name, MAC, IP>	User authentication server invalid.	Error
<Clean Access Server IP> is inaccessible!	Heartbeat between Clean Access Manager and Clean Access Server failed; the Clean Access Server is offline.	Critical error; Clean Access Server should be brought up immediately
Dhcp properties are added	DHCP properties are published to DHCP server in Clean Access Server.	Normal configuration log
Dhcp properties are not added	DHCP properties publishing to Clean Access Server failed.	Error while publishing DHCP properties to the Clean Access Server
Cleared the event log	The entire event log has been cleared.	Normal configuration log
Domain authentication server information not available	User login failed; authentication server information not available.	Error on user login
Domain authentication server information not set	User login failed; authentication server information not completely configured.	Error on user login
<MAC address> added to MAC list	Device MAC address is added to the list.	Normal configuration log
<MAC address> could not be added to the MAC list	Device MAC address is not added to the list.	Error
<MAC address> is already in the MAC list	Device MAC address already added to the list.	Normal configuration log
<MAC address> removed from the MAC list	Device MAC address is removed from the list.	Normal configuration log
Updated policy to <Clean Access Server IP>	Policy is updated successfully.	Normal configuration log
Could not update policy to <Clean Access Server IP>	Policy update to Clean Access Server failed.	Error
Could not update policy to all Clean Access Servers, policies will be published whenever connected	A global policy is not updated to all Clean Access Servers; some of the servers might be disconnected.	Normal configuration log. Not an error, as the policies will be updated when they are connected.
Unable to ping <User IP>, going to logout user <Username>	Ping manager is logging off user, as the user is not online. Automatic user log off feature.	Normal user log
<Role name> role already exists	A role by this name has already been created.	Normal configuration log
<Role Name> role is created successfully	The role has been created successfully.	Normal configuration log
Deleting role <Role Name> failed, Clean Access Server <Clean Access Server IP> is not connected	Deleting role failed; Clean Access Server is not connected.	Error

Table A-1 Event Log Messages (Sheet 3 of 4)

Message	Explanation	Severity
Could not connect to <Clean Access Server IP>	Clean Access Server could not be added to the Clean Access Manager administration domain; the Clean Access Server is offline or not reachable by the Clean Access Manager.	Error
<Clean Access Server IP> added to Clean Access Manager	Clean Access Server is added successfully to the Clean Access Manager administration domain.	Normal configuration log
<Clean Access Server IP> updated in Clean Access Manager	Clean Access Server is updated successfully.	Normal configuration log
<Clean Access Server IP> is not configured in Clean Access Manager	Updating Clean Access Server failed; Clean Access Server information not found in the Clean Access Manager.	Error
<Subnet/Netmask> is already in the SUBNET list	Subnet has already been added to the subnet list.	Normal configuration log
<Subnet/Netmask> removed from the SUBNET list	Subnet is removed from the list successfully.	Normal configuration log

Table A-1 Event Log Messages (Sheet 4 of 4)

Message	Explanation	Severity
<IP Number> System Stats	Runtime statistics for the identified Clean Access Server. The information is: • **load factor** – Current number of packets in the queue that the server is processing (i.e., the current load being handled by the Clean Access Server). • **max since reboot** – The maximum number of packets in the queue at any one time (i.e., the maximum load handled by the Clean Access Server). • **mem** – The memory usage statistics. This lists the used memory, shared memory, buffered memory, and unused memory. • **cpu** – The processor load on the hardware.	N/A
Unable to process Out-of-Band login request from [<MAC address> <IP address>] <username>. Cause: connected device [<MAC address>] not found.	This error message appears when the CAM does not receive appropriate MAC Notification about the client machine. Three common causes for this error condition are: • The SNMP trap syntax from the managed switch is not compatible with the SNMP trap syntax on the CAM. (Ensure the syntax/configuration between the switch and the CAM is consistent.) • The client machine is already connected to a switch port on the Authentication VLAN before the CAM is configured to manage the switch, thus the CAM cannot authenticate the OOB user login request because the CAM is not aware of the client machine connected to the switch port. (Try disconnecting the client machine from the switch port and reconnecting.) • There are one or more device filters acting upon the client machine MAC address and/or the client machine MAC address appears as an exempt device in the CAM's Certified Devices List.	Error



API Support

This chapter discusses API support for the Clean Access Manager. Topics include:

- Overview, page B-1
- Authentication Requirements, page B-2
- Device Filter Operations, page B-3
- Synchronizing with ISE Profiler Operations, page B-7
- Certified Devices List Operations, page B-7
- User Operations, page B-9
- Guest Access Operations, page B-12
- OOB Switch Management Operations, page B-13
- Report Operations, page B-14

Overview

Cisco NAC Appliance provides a utility script called **cisco_api.jsp** that allows you to perform certain operations using HTTPS POST. The actual Cisco NAC Appliance API for your Clean Access Manager is accessed via **https://<cam-IP-or-hostname>/admin/cisco_api.jsp.**

To access the web documentation page for the Cisco NAC Appliance API, login to your CAM web console and type “cisco_api.jsp” after “admin/” in your CAM console’s URL. This will redirect the browser to the web documentation page for the Cisco NAC Appliance API.

Note You must first log into the CAM web console before you can access the cisco_api.jsp documentation page.

To use this API, note the following:

- Competency with a scripting language (e.g. Java, Perl) is required and you must install the scripting software on the machine that runs these scripts.
- Cisco TAC does not support debugging of scripting packages (Java, Perl, etc.)

Note For general information on adding MAC address filters through the CAM web console interface, see Global Device and Subnet Filtering, page 2-10.

Authentication Requirements

Authentication over SSL is required to access the API. Two authentication methods are supported:

- Session-Based Authentication

  With this method, the administrator uses the *adminlogin* and *adminlogout* functions to create a cookie-based session with the server. The *adminlogin* function logs in the admin user and if successful, the HTTP response from the server will contain the session cookie to be used for the duration of the session. The *adminlogout* function logs out the admin user and invalidates the session. However, if the *adminlogout* function is not used, the CAM terminates the session by the configured or default admin session timeout.

- Function-Based Authentication

  If you do not want to used session-based authentication, you can use function-based authentication. With this method, the admin authenticates by passing his or her admin account credentials in every call to the API using the *admin* and *passwd* arguments in the request URL. If authenticating by function, you must add the *admin* and *passwd* parameters to all functions that you are using in your existing script. In this case, you do not use the *adminlogin* and *adminlogout* functions.

Administrator Operations

Use the *adminlogin* and *adminlogout* functions to create a shell script for session-based authentication using a session ID cookie. If you decide not to use session-based authentication, you will need to include the *admin* and *passwd* arguments within each API call instead.

adminlogin

The *adminlogin* function logs in the admin and starts the cookie-based session.

Required In Parameters:

- op: adminlogin
- admin: Administrator account username
- passwd: Administrator account password.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

<any subsequent operation>

The HTTP session cookie obtained through the adminlogin needs to be passed back as part of the HTTP request in any subsequent operation.

Required In Parameters:

- op: <ANY operation>
- <any operation specific parameters>

adminlogout

The *adminlogout* function logs out the administrator and invalidates the session.

Required In Parameters:

- op: adminlogout

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

Device Filter Operations

The following APIs perform operations on the CAM's Device Filter List (devices which bypass the user login requirement).

- addmac, page B-3
- removemac, page B-4
- checkmac, page B-4
- getmaclist, page B-5
- removemaclist, page B-5
- addsubnet, page B-6
- updatesubnet, page B-6
- removesubnet, page B-6

Note See also changeuserrole, page B-11.

addmac

The *addmac* function adds one or more MAC addresses to the Device Filters list.

Required In Parameters:

- op: addmac
- mac: Specifies an exact MAC address or a range.
  Supported formats: 00:01:12:23:34:45 or 00:01:12:* or 00:01:12:23:34:45-11:22:33:44:55:66

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Optional In Parameters:

- ip: Specifies an IPv4 address for an exact MAC address. If you use a wildcard or range to specify a MAC address range, do not use the "ip" parameter. Supported format: 192.168.0.10
- type: Specifies one of the following strings: deny (default), allow, userole, check, or ignore.

- role: Specifies a role name. The role parameter is not required for the unauthenticated role (default) but is required for “userole” or “check”.
- desc: Provides a description.
- ssip: Specifies the IP address used for configuring a Clean Access Server to Clean Access Manager. The default is global.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

removemac

The *removemac* function removes one or more MAC addresses from the Device Filters list.

Required In Parameters:

- op: removemac
- mac: Specifies one or more MAC addresses to delete from the device filters list. The MAC addresses must exactly match the display format including wildcards. You can specify multiple MAC addresses with a comma separated list.

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Optional In Parameter:

- ssip: Specifies the IP address to use for configuring Clean Access Server to Clean Access Manager. The default is global.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

checkmac

The *checkmac* function queries the Device Filters list to check if a particular MAC address exists.

Required In Parameters:

- op: checkmac
- mac: Specifies the MAC address, which must exactly match the display format (00:01:12:23:34:45).

Optional In Parameter:

- ssip: Specifies the Clean Access Server IP address. By default, the *checkmac* function only checks global filters. If ssip provided, the Clean Access Server filters are also checked.

Out Parameters: <!--error=mesg--> comment

- Success:

  Either:

```
<!--error=0-->
<!--found=false-->
```

Or:

```
<!--error=0-->
<!--found=true-->
<!--MAC=0A:13:07:9B:82:60,[IP=x.x.x.x,][CAS=y.y.y.y,]TYPE=ALLOW,[ROLE=zzz,]DESCRIPTION
=My Filter-->
```

In the device filter string:

- "IP=x.x.x.x" is only given for filters with an IP address configured.
- "CAS=y.y.y.y" is only given for server specific filters.
- "ROLE=zzz" is only given for filters with ROLE/CHECK types.
- For a specified single MAC address, the *checkmac* function returns the first matched filters, which can be a single MAC address filter or a MAC address wildcard/range filter.

- Failure: error string

getmaclist

The *getmaclist* function fetches the entire Device Filters list.

Required In Parameter:

- op: getmaclist

Out Parameters: <!--error=mesg--> comment

- Success:

```
<!--error=0-->
<!--count=number_of_filters-->
<!--MAC=0A:13:07:9B:82:60,[IP=x.x.x.x,][CAS=y.y.y.y,]TYPE=ALLOW,[ROLE=zzz,]DESCRIPTION
=My Filter--
...
```

In the device filter string:

- "IP=x.x.x.x" is only given for filters with an IP address configured.
- "CAS=y.y.y.y" is only given for server specific filters.
- "ROLE=zzz" is only given for filters with ROLE/CHECK types.

- Failure: error string

removemaclist

The *removemaclist* function removes the entire Device Filters list.

Required In Parameter:

- op: removemaclist

Out Parameters:

- For unsuccessful operation, the output is <!--error=mesg-->
- For successful operation, the output is <!--error=0-->

addsubnet

The *addsubnet* function adds a subnet to the Devices list.

Required In Parameters:

- op: addsubnet
- subnet: Supported formats a.b.c.d for subnet address. e.g.: subnet=10.210.0.0
- mask: Mask in CIDR format. e.g.: mask=16.

Optional In Parameters:

- type: One of the Strings [deny, allow, userole]. Default is deny.
- role: Specify role name. Default is unauthenticated. Required if type is userole.
- desc: Any description string.
- ssip: Default is global. Provide the IP address used for configuring Clean Access Server to Clean Access Manager.

Out Parameters:

Comment of form <!--error=mesg--> is returned. If mesg value is 0 then operation is success or else there will be an error string.

updatesubnet

The *updatesubnet* function updates a Subnet entry in Devices list.

Required In Parameters:

- op: updatesubnet
- subnet: Supported formats a.b.c.d for subnet address. e.g.: subnet=10.210.0.0
- mask: Mask in CIDR format. e.g.: mask=16.

Optional In Parameters:

- type: One of the Strings [deny, allow, userole]. Default is deny.
- role: Specify role name. Default is unauthenticated. Required if type is userole.
- desc: Any description string.
- ssip: Default is global. Provide the IP address used for configuring Clean Access Server to Clean Access Manager.

Out Parameters:

Comment of form <!--error=mesg--> is returned. If mesg value is 0 then operation is success or else there will be an error string.

removesubnet

The *removesubnet* function removes a subnet entry from the Devices list.

Required In Parameters:

- op: removesubnet
- subnet: Supported formats a.b.c.d for subnet address (e.g. subnet=10.210.0.0)

- mask: Mask in CIDR format (e.g.: mask=16)

Optional In Parameter:

- ssip: Default is global. Provide the IP address used for configuring Clean Access Server to Clean Access Manager.

Synchronizing with ISE Profiler Operations

The following API commands are used while synchronizing Cisco ISE Profiler endpoints with NAC Manager.

- profilerEndpointEvent, page B-7
- resyncwithprofiler, page B-7

profilerEndpointEvent

The *profilerEndpointEvent* adds, updates, or deletes endpoints from Cisco ISE to NAC Manager.

Required In Parameters:

- op: profilerEndpointEvent
- action: Specifies the action to be performed with the endpoints: add, update, delete.
- xmlString: Contains the details of endpoints.

Out Parameters:

- Success: The endpoints are successfully added, updated, or deleted accordingly.
- Failure: error string returned as “Invalid action specified for the profiler event: {action}. Allowed action types are: add, delete and update.”

resyncwithprofiler

The *resyncwithprofiler* is used to re-synchronize NAC Manager with endpoints in Cisco ISE.

Required In Parameters:

- op: resyncwithprofiler

Out Parameters:

- Success: All the ISE endpoints are synchronized with NAC Manager.
- Failure: error string returned as “Exception while adding a resync with profiler job.{Reason}”

Certified Devices List Operations

The following APIs perform actions on the Certified Device list (devices which have met posture assessment requirements).

- addcleanmac, page B-8
- removecleanmac, page B-8

- clearcertified, page B-9

addcleanmac

The *addcleanmac* function adds one or more MAC addresses to the Certified Devices list as exempted devices.

Required In Parameters:

- op: addcleanmac
- mac: Specifies the MAC addresses to add. Supported formats 00:01:12:23:34:45 or 00-01-12-23-34-45 or 000112233445

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Optional In Parameter:

- ssip: Default is global. Specifies the IP address used for configuring Clean Access Server to Clean Access Manager.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

removecleanmac

The *removecleanmac* function removes one or more MAC addresses from the Certified Devices list.

Required In Parameters:

- op: removecleanmac
- mac: Specifies one or more MAC addresses to remove. Supported formats 00:01:12:23:34:45 or 00-01-12-23-34-45 or 000112233445

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Optional In Parameter:

- ssip: Default is global. Provide the IP address used for configuring Clean Access Server to Clean Access Manager.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: one or more error strings can appear if ssip is not provided and if a MAC address cannot be deleted from more than one Clean Access Server.

clearcertified

The *clearcertified* function deletes all of the existing entries from the Clean Access Certified Devices list.

Required In Parameter:

- op: clearcertified

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

User Operations

The following APIs perform user management operations:

- kickuser, page B-9
- kickuserbymac, page B-10
- kickoobuser, page B-10
- queryuserstime, page B-10
- renewuserstime, page B-11
- changeuserrole, page B-11
- changeloggedinuserrole, page B-11

Note See also getlocaluserlist, page B-12, addlocaluser, page B-13, and deletelocaluser, page B-13.

kickuser

The *kickuser* function terminates the active session of one or more currently logged-in In-Band users, and removes the user from the In-Band Online Users list.

Required In Parameters:

- op: kickuser
- ip: Specifies one IP address or a comma separated list of IP addresses.

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0

- Failure: error string

kickuserbymac

The *kickuserbymac* function terminates the active session by MAC address of one or more logged-in In-Band users and removes the user(s) from the In-Band Online Users list.

Required In Parameters:

- op: kickuserbymac
- mac: Specifies one MAC address or a comma separated list of MAC addresses.

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

kickoobuser

The *kickoobuser* function terminates the active session of one or more OOB users and removes the user(s) from the Out-of-Band Online Users list.

Required In Parameters:

- op: kickoobuser
- mac: Specifies a MAC address or a comma separated list of MAC addresses.

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

queryuserstime

The *queryuserstime* function queries the remaining session time for logged-in users. This function returns a list of logged-in users in roles with configured session timeouts.

Required In Parameters:

- op: queryuserstime

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; another <!--list=iplist--> comment with an IP list and session time remaining for each IP entry
- Failure: error string

renewuserstime

The *renewuserstime* function renews the logged-in In-Band users session timeout by a session.

Required In Parameters:

- op: renewuserstime
- list: Specifies a comma-separated list of IP addresses. Supported format: 10.1.10.10, 10.1.10.11, 10.1.10.12

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

changeuserrole

The *changeuserrole* function changes In-Band user access permissions for a logged-in user by removing the user from the Online Users list and adding the user's MAC address to the Device Filters list with a new role.

Required In Parameters:

- op: changeuserrole
- ip: Specifies the IP address of a user who is logged in.
- role: Specifies the role to which the user is to be moved.

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

changeloggedinuserrole

The *changeloggedinuserrole* function changes access permissions for a logged-in In-Band user by changing that user's current role to a new role.

Required In Parameters:

- op: changeloggedinuserrole
- ip: Specifies the IP address of a logged-in user. To specify multiple users, use a comma-separated IP list.
- role: Specifies a new role for the user.

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

Guest Access Operations

The following APIs allow administrators to create, delete, and view local user accounts on the CAM:

- getlocaluserlist, page B-12
- addlocaluser, page B-13
- deletelocaluser, page B-13

Local users are those internally validated by the CAM as opposed to an external authentication server. These APIs are intended to support guest access for dynamic token user access generation, providing the ability to:

- Use a webpage to access Cisco NAC Appliance API to insert a visitor username/password combination, such as jdoe@visitor.com/jdoe112805, and then assign a role, such as *guest1day*.
- Delete all guest users associated with the guest access role for that day.
- List all usernames associated with the guest access role.

These APIs support most implementations of guest user access dynamic token/password generation and allow the removal of those users for a guest role.

You must create the front-end generation password/token. For accounting purposes, Cisco NAC Appliance provides RADIUS accounting functionality only.

getlocaluserlist

The *getlocaluserlist* function returns a list of local user accounts with user name and role name.

Required In Parameters:

- op: getlocaluserlist

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; <!--count=10--> shows the number of users returned and is followed by same number of comments of form <!--NAME=jdoe,ROLE=Student-->
- Failure: error string

addlocaluser

The *addlocaluser* function adds a new local user account.

Required In Parameters:

- op: addlocaluser
- username: Specifies a new local user account user name.
- userpass: Specifies the user password for the new local user account.
- userrole: Specifies the role for the new local user account.

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

deletelocaluser

The *deletelocaluser* function deletes one or all local user accounts.

Required In Parameters:

- op: deletelocaluser
- qtype: Specifies the data type: 'name' or 'all'
- qval: Specifies the exact username in single quotes or an empty string (‘’) to indicate “all.”

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0
- Failure: error string

OOB Switch Management Operations

You can manage switch ports to which users are connected with the following OOB management functions:

- bounceport, page B-14

- bounceportbymac, page B-14

bounceport

The *bounceport* function bounces an OOB port in a switch that a client connects to given the switch ID and port number.

Required In Parameters:

- op: bounceport
- switch: ID of the switch as inserted in the CAM DB table ‘switch’.
- port: OOB Port in the switch to be bounced.

Out Parameters:

Comment of form <!--error=mesg--> is returned. If mesg value is 0 then operation is success or else there will be an error string.

bounceportbymac

The *bounceportbymac* function bounces an OOB port in a switch that a client connects to given the mac address of the connected device

Required In Parameters:

- op: bounceportbymac
- mac: Provide MAC address of the connected device whose port of connection in any associated switch has to be bounced.

Out Parameters:

Comment of form <!--error=mesg--> is returned. If mesg value is 0 then operation is success or else there will be an error string.

Report Operations

You can create scripts to compile lists of information or reports with the following report functions:

- getversion, page B-15
- getuserinfo, page B-15
- getoobuserinfo, page B-16
- getcleanuserinfo, page B-16
- getreports, page B-16
- getuallist, page B-21
- getualfile, page B-21
- getcannedreportslist, page B-22
- getcannedreport, page B-22

getversion

The *getversion* function returns the version number of the CAM.

Required In Parameters:

- op: getversion

Out Params:

- Comment of form <!--version=version--> is returned.

getuserinfo

Given an IP address, MAC address, or username, the *getuserinfo* function retrieves the following user information:

- *IP* in IPv4 format
- MAC address
- *Name* is the username
- *Provider* can be the LDAP server
- *Role* is the current role assigned to the user
- *Origrole* is the original role assigned to the user
- *VLAN* is the original VLAN tag
- *NEWVLAN* is the current VLAN tag
- Operating system of the user's system

If multiple users match the criteria, the system returns a list of users. If you enter "all" as the qtype Parameter, all information for all users is retrieved.

Required In Parameters:

- op: getuserinfo
- qtype: Specifies one of the following strings: ip, mac, name, or all.
- qval: Specifies an IP address, MAC address, or username depending on the qtype parameter; enter an empty string ('') to indicate "all."

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; <!--count=10--> shows the number of users returned and is followed by a corresponding number of comments <!--IP=10.1.10.12,MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,ORIGROLE=Student,VLAN=1024,NEWVLAN=1024,OS=Windows XP-->
- Failure: error string

getoobuserinfo

Given an IP address, MAC address or username, the *getoobuserinfo* function retrieves information about the logged-in Out-of-Band (OOB) users, or given the qtype "all", the system generates a list of information about all logged-in OOB users. If multiple users match the criteria, the system generates a list of users.

Required In Parameters:

- op: getoobuserinfo
- qtype: Specifies the method of identifying one or more users: ip, mac, name, all.
- qval: Specifies an IP or MAC address or a username; enter an empty string ('') to indicate "all".

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; <!--count=10--> shows the number of users returned and is followed by a matching number of comments of form <!--IP=10.1.10.12,MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,AUTHVLAN=10,ACCESSVLAN=1024,OS=Windows XP,SWITCHIP=10.1.10.1,PORTNUM=18-->
- Failure: error string

getcleanuserinfo

Given a MAC address or username, the *getcleanuserinfo* function returns information about certified users. If there are multiple users matching the criteria, the system generates a list of certified users.

Required In Parameters:

- op: getcleanuserinfo
- qtype: Specifies the method of identifying the user: mac, name, all.
- qval: Specifies MAC address or username; enter an empty string ('') to indicate "all."

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; <!--count=10--> shows the number of users returned and is followed by a matching number of comments of form <!--MAC=0A:13:07:9B:82:60,NAME=jdoe,PROVIDER=LDAP Server,ROLE=Student,VLAN=10-->
- Failure: error string

getreports

The *getreports* function returns a report that contains customized content. You can also use this function to compile a list of users with certain software installed.

Required In Parameters:

op: getreports

Note If you do not use session-based authentication, the *admin* and *passwd* arguments are required. See Authentication Requirements, page B-2.

Optional Query Parameters:

Table B-1 lists the query Parameters for the *getreports* function.

Table B-1 Query Parameters for the getreports function

Parameter Name	Allowed Values	Description
status	One of the following values: • any (default) • success • failure	Reports only information for the specified status.
user	A string; empty single quotes (‘’) is the default	Reports information about the specified user.
agentType	One of the following values: • any (default) • web • win • mac	Reports information originating from the specified Cisco NAC Appliance Agent type.
ip	One valid IPv4 address, such as 10.20.30.40; empty single quotes is the default	Reports information about the specified IP address.
mac	One valid MAC address, such as 00:01:12:23:34:45; empty single quotes is the default	Reports information about the specified MAC address.

Table B-1 Query Parameters for the getreports function (continued)

Parameter Name	Allowed Values	Description
os	One of the following values: • To indicate any OS, enter empty single quotes (‘’) (default) • WINDOWS_ALL (Windows (All)) • WINDOWS_8_ALL (Windows 8 (All)) • WINDOWS_7_ALL (Windows 7 (All)) • WINDOWS_7_STARTER (Windows 7 Starter) • WINDOWS_7_HOME_BASIC (Windows 7 Home Basic) • WINDOWS_7_HOME_PREMIUM (Windows 7 Home Premium) • WINDOWS_7_PROFESSIONAL (Windows 7 Professional) • WINDOWS_7_ENTERPRISE (Windows 7 Enterprise) • WINDOWS_7_ULTIMATE (Windows 7 Ultimate) • WINDOWS_7_64_HOME_BASIC (Windows 7 Home Basic x64) • WINDOWS_7_64_HOME_PREMIUM (Windows 7 Home Premium x64) • WINDOWS_7_64_PROFESSIONAL (Windows 7 Professional x64) • WINDOWS_7_64_ENTERPRISE (Windows 7 Enterprise x64)	Reports information about the specified OS.

Table B-1 Query Parameters for the getreports function (continued)

Parameter Name	Allowed Values	Description
os (continued)	• WINDOWS_7_64_ULTIMATE (Windows 7 Ultimate x64) • WINDOWS_VISTA_ALL (Windows Vista (all)) • WINDOWS_VISTA_HOME_BASIC (Windows Vista Home Basic) • WINDOWS_VISTA_HOME_PREMIUM (Windows Vista Home Premium) • WINDOWS_VISTA_BUSINESS (Windows Vista Business) • WINDOWS_VISTA_ULTIMATE (Windows Vista Ultimate) • WINDOWS_VISTA_ENTERPRISE (Windows Vista Enterprise) • WINDOWS_VISTA_64_HOME_BASIC (Windows Vista Home Basic x64) • WINDOWS_VISTA_64_HOME_PREMIUM (Windows Vista Home Premium x64) • WINDOWS_VISTA_64_BUSINESS (Windows Vista Business x64) • WINDOWS_VISTA_64_ULTIMATE (Windows Vista Ultimate x64) • WINDOWS_VISTA_64_ENTERPRISE (Windows Vista Enterprise x64) • WINDOWS_XP (Windows XP (All)) • WINDOWS_PRO_XP (Windows XP Pro/Home) • WINDOWS_TPC_XP (Windows XP Tablet PC Edition) • WINDOWS_MCE_XP (Windows XP Media Center Edition) • MAC_OSX (Mac OS (all)) • MAC_OS_10_5 (Mac OS 10.5) • MAC_OS_10_6 (Mac OS 10.6) • MAC_OS_64_10_6 (Mac OS 10.6 x64)	Reports information about the specified OS.

Table B-1 Query Parameters for the getreports function (continued)

Parameter Name	Allowed Values	Description
timeRange	timeFrom, timeTo • timeFrom can be one of the following values: – timestamp (format: yyyy-mm-dd hh:mm:ss) – negative integer representing the number of hours before now – past • timeTo can be one of the following values: – timestamp (format: yyyy-mm-dd hh:mm:ss) – negative integer representing the number of hours before now – now – -48, -24 (the day before last) – -24, now (within last day) – 2007-01-01 00:00:00, 2007-02-28 23:59:59 (Between Jan 1st and Feb 28th) Default: past, now (any time: all possible reports)	Reports information collected within the specified time range.
showText	One of the following values: • true— Returns the text. • false—Does not return the text. (default)	Indicates whether or not to return the report text.
orderBy	One of the following values: • user • ip • mac • os • time (default)	Specifies the report organization.
orderDir	One of the following values: • asc—Indicates ascending order. (default) • desc—Indicates descending order.	Specifies ascending or descending order for the data.
instSoft	One of the following values: • Empty single quotes (‘’) indicates “any” (default) • AV—Indicates AntiVirus installed • AS—Indicates AntiSpyware installed • UNKNOWN AV/AS—Indicates an unknown AV/AS	Restricts to reports containing this type of installed software.

Table B-1 Query Parameters for the getreports function (continued)

Parameter Name	Allowed Values	Description
reqName	Name of the AV or AS software requirement; empty quotes “any” (default)	Restricts to reports containing this software requirement.
reqStatus	One of the following values: • any (default) • success • failure	Restricts to reports where the software requirement is of this status (only if reqName is used).

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; <!--count=count--> shows the number of reports returned; the reports follow the count comment and are of the form: <!--status=status,user=user,agentType=agentType,ip=ip,mac=mac,os=os,time=time,text=text-->
- Failure: error string

getuallist

The *getuallist* function fetches the list of XML data files stored in **/perfigo/control/data/logs/ual**.

Required In Parameter:

- op: getuallist
- admin: Administrator account username
- passwd: Administrator account password
- ip: Specifies IP Address of the Cisco NAC Appliance API (**https://<cam-IP-or-hostname>/admin/cisco_api.jsp)**

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; <!--count=count--> shows the number of files returned; the list of filenames follow the count comment and are of the form: <!--filename=filename-->
- Failure: error string

getualfile

The *getualfile* function displays the contents of the specified UAL file.

Required In Parameter:

- op: getUALfile
- filename: Specifies the UAL file name
- admin: Administrator account username
- passwd: Administrator account password
- ip: Specifies IP Address of the Cisco NAC Appliance API (**https://<cam-IP-or-hostname>/admin/cisco_api.jsp)**

Out Parameters:

The contents of the specified file name are displayed.

getcannedreportslist

The *getcannedreportslist* function fetches the list of all the canned report files in the canned directory: **/perfigo/control/data/reports**.

Required In Parameter:

- op: getcannedreportslist
- admin: Administrator account username
- passwd: Administrator account password
- ip: Specifies IP Address of the Cisco NAC Appliance API (**https://<cam-IP-or-hostname>/admin/cisco_api.jsp)**

Out Parameters: <!--error=mesg--> comment

- Success: mesg value of 0; <!--count=count--> shows the number of reorts returned; the reports follow the count comment and are of the form: <!--filename=filename-->
- Failure: error string

getcannedreport

The *getcannedreport* function displays the contents of specified canned report file.

Required In Parameter:

- op: getcannedreport
- filename: Specifies the canned report file name
- admin: Administrator account username
- passwd: Administrator account password
- ip: Specifies IP Address of the Cisco NAC Appliance API (**https://<cam-IP-or-hostname>/admin/cisco_api.jsp)**

Out Parameters:

The contents of the specified file name are displayed.



MIB Support

This chapter lists Objects and Object Identifiers (OIDs) for the Management Information Base (MIBs) supported by Clean Access Manager.

- CLEAN ACCESS - MIB
- SNMPv2-MIB
- RFC1213-MIB
- IP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB
- MTA-MIB
- IF-MIB
- DISMAN-EVENT-MIB
- NOTIFICATION-LOG-MIB
- UCD-SNMP-MIB
- UCD-DLMOD-MIB
- NET-SNMP-AGENT-MIB
- SNMPv2-SMI
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-TARGET-MIB
- SNMP-USER-BASED-SM-MIB
- SNMP-VIEW-BASED-ACM-MIB

Table C-1 CLEAN ACCESS - MIB

Object	OID	Description
hostname	1.3.6.1.4.1.16344.1.1.0	Hostname of the Clean Access Manager
cleanaccessIpAddr	1.3.6.1.4.1.16344.1.2.0	The IP address that the web console is bound to

Table C-1 CLEAN ACCESS - MIB

Object	OID	Description
cleanaccessPort	1.3.6.1.4.1.16344.1.3.0	The port, the web management console is listening on
versionString	1.3.6.1.4.1.16344.1.4.0	Version of Software running on the Clean Access Manager
cleanaccessServerCount	1.3.6.1.4.1.16344.1.5.0	Number of Clean Access Servers managed by this Clean Access Manager
alertCount	1.3.6.1.4.1.16344.1.6.0	Number of Alerts
cleanaccessServerTable	1.3.6.1.4.1.16344.1.7	
cleanaccessServerEntry	1.3.6.1.4.1.16344.1.7.1	
cleanaccessServerTableIndex	1.3.6.1.4.1.16344.1.7.1.1	A number identifying this cleanaccessServerTable entry
cleanaccessServerTableIpAddress	1.3.6.1.4.1.16344.1.7.1.2	The IP address of the Clean Access Server
cleanaccessServerTableLocation	1.3.6.1.4.1.16344.1.7.1.3	The location of Clean Access Server
cleanaccessServerTableVersion	1.3.6.1.4.1.16344.1.7.1.4	Clean Access Server version
cleanaccessServerTableType	1.3.6.1.4.1.16344.1.7.1.5	The deployment type of the Clean Access Server
cleanaccessServerTableRowStatus	.1.3.6.1.4.1.16344.1.7.1.6	An existing row in the table
nodeActive	1.3.6.1.4.1.16344.0.8	Alert sent when this node becomes active in High Availability mode
nodeStandby	1.3.6.1.4.1.16344.0.9	Alert sent when this node becomes standby in High Availability mode
nodeShutdown	1.3.6.1.4.1.16344.0.10	Alert sent when this node is being administratively shutdown
adssoStarted	1.3.6.1.4.1.16344.0.11	ADSSO service started
adssoStopped	1.3.6.1.4.1.16344.0.12	ADSSO service stopped
Objects not supported in Clean Access- MIB		
Object	**OID**	
alertTable	1.3.6.1.4.1.16344.1.8	
alertEntry	1.3.6.1.4.1.16344.1.8.1	
alertTableIndex	1.3.6.1.4.1.16344.1.8.1.1	
alertTableType	1.3.6.1.4.1.16344.1.8.1.2	
alertTableTime	1.3.6.1.4.1.16344.1.8.1.3	
alertTableStatus	1.3.6.1.4.1.16344.1.8.1.4	

Table C-1 CLEAN ACCESS - MIB

Object	OID	Description
alertTableText	1.3.6.1.4.1.16344.1.8.1.5	
alertTableRowStatus	1.3.6.1.4.1.16344.1.8.1.6	

Table C-2 SNMPv2-MIB

Object	OID
sysDescr	1.3.6.1.2.1.1.1
sysObjectID	1.3.6.1.2.1.1.2
sysUpTime	1.3.6.1.2.1.1.3
sysContact	1.3.6.1.2.1.1.4
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6
sysORLastChange	1.3.6.1.2.1.1.8
sysORID	1.3.6.1.2.1.1.9.1.2
sysORDescr	1.3.6.1.2.1.1.9.1.3
sysORUpTime	1.3.6.1.2.1.1.9.1.4

Table C-3 RFC1213-MIB

Object	OID
ifNumber	1.3.6.1.2.1.2.1
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifMtu	1.3.6.1.2.1.2.2.1.4
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8
ifLastChange	1.3.6.1.2.1.2.2.1.9
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15
ifOutOctets	1.3.6.1.2.1.2.2.1.16

Table C-3 RFC1213-MIB (continued)

Object	OID
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19
ifOutErrors	1.3.6.1.2.1.2.2.1.20
ifOutQLen	1.3.6.1.2.1.2.2.1.21
ifSpecific	1.3.6.1.2.1.2.2.1.22

Table C-4 IP-MIB

Object	OID
ipForwarding	1.3.6.1.2.1.4.1
ipDefaultTTL	1.3.6.1.2.1.4.2
ipInReceives	1.3.6.1.2.1.4.3
ipInHdrErrors	1.3.6.1.2.1.4.4
ipInAddrErrors	1.3.6.1.2.1.4.5
ipForwDatagrams	1.3.6.1.2.1.4.6
ipInUnknownProtos	1.3.6.1.2.1.4.7
ipInDiscards	1.3.6.1.2.1.4.8
ipInDelivers	1.3.6.1.2.1.4.9
ipOutRequests	1.3.6.1.2.1.4.10
ipOutDiscards	1.3.6.1.2.1.4.11
ipOutNoRoutes	1.3.6.1.2.1.4.12
ipReasmTimeout	1.3.6.1.2.1.4.13
ipReasmReqds	1.3.6.1.2.1.4.14
ipReasmOKs	1.3.6.1.2.1.4.15
ipReasmFails	1.3.6.1.2.1.4.16
ipFragOKs	1.3.6.1.2.1.4.17
ipFragFails	1.3.6.1.2.1.4.18
ipFragCreates	1.3.6.1.2.1.4.19
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4
ipRouteDest	1.3.6.1.2.1.4.21.1.1
ipRouteIfIndex	1.3.6.1.2.1.4.21.1.2
ipRouteMetric1	1.3.6.1.2.1.4.21.1.3
ipRouteNextHop	1.3.6.1.2.1.4.21.1.7

Table C-4 IP-MIB (continued)

Object	OID
ipRouteType	1.3.6.1.2.1.4.21.1.8
ipRouteProto	1.3.6.1.2.1.4.21.1.9
ipRouteMask	1.3.6.1.2.1.4.21.1.11
ipRouteInfo	1.3.6.1.2.1.4.21.1.13
ipNetToMediaIfIndex	1.3.6.1.2.1.4.22.1.1
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3
ipNetToMediaType	1.3.6.1.2.1.4.22.1.4
ipRoutingDiscards	1.3.6.1.2.1.4.23
ipCidrRouteDest	1.3.6.1.2.1.4.24.4.1.1
ipCidrRouteMask	1.3.6.1.2.1.4.24.4.1.2
ipCidrRouteTos	1.3.6.1.2.1.4.24.4.1.3
ipCidrRouteNextHop	1.3.6.1.2.1.4.24.4.1.4
ipCidrRouteIfIndex	1.3.6.1.2.1.4.24.4.1.5
ipCidrRouteType	1.3.6.1.2.1.4.24.4.1.6
ipCidrRouteProto	1.3.6.1.2.1.4.24.4.1.7
ipCidrRouteInfo	1.3.6.1.2.1.4.24.4.1.9
ipCidrRouteNextHopAS	1.3.6.1.2.1.4.24.4.1.10
ipCidrRouteMetric1	1.3.6.1.2.1.4.24.4.1.11
ipCidrRouteMetric2	1.3.6.1.2.1.4.24.4.1.12
ipCidrRouteMetric3	1.3.6.1.2.1.4.24.4.1.13
ipCidrRouteMetric4	1.3.6.1.2.1.4.24.4.1.14
ipCidrRouteMetric5	1.3.6.1.2.1.4.24.4.1.15
ipCidrRouteStatus	1.3.6.1.2.1.4.24.4.1.16
inetCidrRouteNumber	1.3.6.1.2.1.4.24.6
inetCidrRouteIfIndex	1.3.6.1.2.1.4.24.7.1.7
inetCidrRouteType	1.3.6.1.2.1.4.24.7.1.8
inetCidrRouteProto	1.3.6.1.2.1.4.24.7.1.9
inetCidrRouteAge	1.3.6.1.2.1.4.24.7.1.10
inetCidrRouteNextHopAS	1.3.6.1.2.1.4.24.7.1.11
inetCidrRouteMetric1	1.3.6.1.2.1.4.24.7.1.12
inetCidrRouteMetric2	1.3.6.1.2.1.4.24.7.1.13
inetCidrRouteMetric3	1.3.6.1.2.1.4.24.7.1.14
inetCidrRouteMetric4	1.3.6.1.2.1.4.24.7.1.15
inetCidrRouteMetric5	1.3.6.1.2.1.4.24.7.1.16
inetCidrRouteStatus	1.3.6.1.2.1.4.24.7.1.17

Table C-4 IP-MIB (continued)

Object	OID
ipv4InterfaceTableLastChange	1.3.6.1.2.1.4.27
ipv4InterfaceReasmMaxSize	1.3.6.1.2.1.4.28.1.2
ipv4InterfaceEnableStatus	1.3.6.1.2.1.4.28.1.3
ipv4InterfaceRetransmitTime	1.3.6.1.2.1.4.28.1.4
ipv6InterfaceTableLastChange	1.3.6.1.2.1.4.29
ipSystemStatsInReceives	1.3.6.1.2.1.4.31.1.1.3
ipSystemStatsHCInReceives	1.3.6.1.2.1.4.31.1.1.4
ipSystemStatsInHdrErrors	1.3.6.1.2.1.4.31.1.1.7
ipSystemStatsInNoRoutes	1.3.6.1.2.1.4.31.1.1.8
ipSystemStatsInAddrErrors	1.3.6.1.2.1.4.31.1.1.9
ipSystemStatsInUnknownProtos	1.3.6.1.2.1.4.31.1.1.10
ipSystemStatsInTruncatedPkts	1.3.6.1.2.1.4.31.1.1.11
ipSystemStatsInForwDatagrams	1.3.6.1.2.1.4.31.1.1.12
ipSystemStatsHCInForwDatagrams	1.3.6.1.2.1.4.31.1.1.13
ipSystemStatsReasmReqds	1.3.6.1.2.1.4.31.1.1.14
ipSystemStatsReasmOKs	1.3.6.1.2.1.4.31.1.1.15
ipSystemStatsReasmFails	1.3.6.1.2.1.4.31.1.1.16
ipSystemStatsInDiscards	1.3.6.1.2.1.4.31.1.1.17
ipSystemStatsInDelivers	1.3.6.1.2.1.4.31.1.1.18
ipSystemStatsHCInDelivers	1.3.6.1.2.1.4.31.1.1.19
ipSystemStatsOutRequests	1.3.6.1.2.1.4.31.1.1.20
ipSystemStatsHCOutRequests	1.3.6.1.2.1.4.31.1.1.21
ipSystemStatsOutNoRoutes	1.3.6.1.2.1.4.31.1.1.22
ipSystemStatsOutForwDatagrams	1.3.6.1.2.1.4.31.1.1.23
ipSystemStatsHCOutForwDatagrams	1.3.6.1.2.1.4.31.1.1.24
ipSystemStatsOutDiscards	1.3.6.1.2.1.4.31.1.1.25
ipSystemStatsOutFragReqds	1.3.6.1.2.1.4.31.1.1.26
ipSystemStatsOutFragOKs	1.3.6.1.2.1.4.31.1.1.27
ipSystemStatsOutFragFails	1.3.6.1.2.1.4.31.1.1.28
ipSystemStatsOutFragCreates	1.3.6.1.2.1.4.31.1.1.29
ipSystemStatsOutTransmits	1.3.6.1.2.1.4.31.1.1.30
ipSystemStatsHCOutTransmits	1.3.6.1.2.1.4.31.1.1.31
ipSystemStatsInMcastPkts	1.3.6.1.2.1.4.31.1.1.34
ipSystemStatsHCInMcastPkts	1.3.6.1.2.1.4.31.1.1.35
ipSystemStatsOutMcastPkts	1.3.6.1.2.1.4.31.1.1.38
ipSystemStatsHCOutMcastPkts	1.3.6.1.2.1.4.31.1.1.39

Table C-4 IP-MIB (continued)

Object	OID
ipSystemStatsInBcastPkts	1.3.6.1.2.1.4.31.1.1.42
ipSystemStatsHCInBcastPkts	1.3.6.1.2.1.4.31.1.1.43
ipSystemStatsOutBcastPkts	1.3.6.1.2.1.4.31.1.1.44
ipSystemStatsHCOutBcastPkts	1.3.6.1.2.1.4.31.1.1.45
ipSystemStatsDiscontinuityTime	1.3.6.1.2.1.4.31.1.1.46
ipSystemStatsRefreshRate	1.3.6.1.2.1.4.31.1.1.47
ipIfStatsTableLastChange	1.3.6.1.2.1.4.31.2
ipAddressPrefixOrigin	1.3.6.1.2.1.4.32.1.5
ipAddressPrefixOnLinkFlag	1.3.6.1.2.1.4.32.1.6
ipAddressPrefixAutonomousFlag	1.3.6.1.2.1.4.32.1.7
ipAddressPrefixAdvPreferredLifetime	1.3.6.1.2.1.4.32.1.8
ipAddressPrefixAdvValidLifetime	1.3.6.1.2.1.4.32.1.9
ipAddressIfIndex	1.3.6.1.2.1.4.34.1.3
ipAddressType	1.3.6.1.2.1.4.34.1.4
ipAddressPrefix	1.3.6.1.2.1.4.34.1.5
ipAddressOrigin	1.3.6.1.2.1.4.34.1.6
ipAddressStatus	1.3.6.1.2.1.4.34.1.7
ipAddressCreated	1.3.6.1.2.1.4.34.1.8
ipAddressLastChanged	1.3.6.1.2.1.4.34.1.9
ipAddressRowStatus	1.3.6.1.2.1.4.34.1.10
ipAddressStorageType	1.3.6.1.2.1.4.34.1.11
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4
ipNetToPhysicalType	1.3.6.1.2.1.4.35.1.6
ipNetToPhysicalState	1.3.6.1.2.1.4.35.1.7
ipNetToPhysicalRowStatus	1.3.6.1.2.1.4.35.1.8
ipDefaultRouterLifetime	1.3.6.1.2.1.4.37.1.4
ipDefaultRouterPreference	1.3.6.1.2.1.4.37.1.5

Table C-5 UDP-MIB

Object	OID
udpEndpointProcess	1.3.6.1.2.1.7.7.1.8

Table C-6 HOST-RESOURCES-MIB

Object	OID
hrSystemUptime	1.3.6.1.2.1.25.1.1
hrSystemDate	1.3.6.1.2.1.25.1.2

Table C-6 HOST-RESOURCES-MIB (continued)

Object	OID
hrSystemInitialLoadDevice	1.3.6.1.2.1.25.1.3
hrSystemInitialLoadParameters	1.3.6.1.2.1.25.1.4
hrSystemNumUsers	1.3.6.1.2.1.25.1.5
hrSystemProcesses	1.3.6.1.2.1.25.1.6
hrSystemMaxProcesses	1.3.6.1.2.1.25.1.7
hrMemorySize	1.3.6.1.2.1.25.2.2
hrStorageIndex	1.3.6.1.2.1.25.2.3.1.1
hrStorageType	1.3.6.1.2.1.25.2.3.1.2
hrStorageDescr	1.3.6.1.2.1.25.2.3.1.3
hrStorageAllocationUnits	1.3.6.1.2.1.25.2.3.1.4
hrStorageSize	1.3.6.1.2.1.25.2.3.1.5
hrStorageUsed	1.3.6.1.2.1.25.2.3.1.6
hrDeviceIndex	1.3.6.1.2.1.25.3.2.1.1
hrDeviceType	1.3.6.1.2.1.25.3.2.1.2
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceID	1.3.6.1.2.1.25.3.2.1.4
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5
hrDeviceErrors	1.3.6.1.2.1.25.3.2.1.6
hrProcessorFrwID	1.3.6.1.2.1.25.3.3.1.1
hrProcessorLoad	1.3.6.1.2.1.25.3.3.1.2
hrNetworkIfIndex	1.3.6.1.2.1.25.3.4.1.1
hrDiskStorageAccess	1.3.6.1.2.1.25.3.6.1.1
hrDiskStorageMedia	1.3.6.1.2.1.25.3.6.1.2
hrDiskStorageRemoveble	1.3.6.1.2.1.25.3.6.1.3
hrDiskStorageCapacity	1.3.6.1.2.1.25.3.6.1.4
hrPartitionIndex	1.3.6.1.2.1.25.3.7.1.1
hrPartitionLabel	1.3.6.1.2.1.25.3.7.1.2
hrPartitionID	1.3.6.1.2.1.25.3.7.1.3
hrPartitionSize	1.3.6.1.2.1.25.3.7.1.4
hrPartitionFSIndex	1.3.6.1.2.1.25.3.7.1.5
hrFSIndex	1.3.6.1.2.1.25.3.8.1.1
hrFSMountPoint	1.3.6.1.2.1.25.3.8.1.2
hrFSRemoteMountPoint	1.3.6.1.2.1.25.3.8.1.3
hrFSType	1.3.6.1.2.1.25.3.8.1.4
hrFSAccess	1.3.6.1.2.1.25.3.8.1.5
hrFSBootable	1.3.6.1.2.1.25.3.8.1.6

Table C-6 HOST-RESOURCES-MIB (continued)

Object	OID
hrFSStorageIndex	1.3.6.1.2.1.25.3.8.1.7
hrFSLastFullBackupDate	1.3.6.1.2.1.25.3.8.1.8
hrFSLastPartialBackupDate	1.3.6.1.2.1.25.3.8.1.9
hrSWRunIndex	1.3.6.1.2.1.25.4.2.1.1
hrSWRunName	1.3.6.1.2.1.25.4.2.1.2
hrSWRunID	1.3.6.1.2.1.25.4.2.1.3
hrSWRunPath	1.3.6.1.2.1.25.4.2.1.4
hrSWRunParameters	1.3.6.1.2.1.25.4.2.1.5
hrSWRunType	1.3.6.1.2.1.25.4.2.1.6
hrSWRunStatus	1.3.6.1.2.1.25.4.2.1.7
hrSWRunPerfCPU	1.3.6.1.2.1.25.5.1.1.1
hrSWRunPerfMem	1.3.6.1.2.1.25.5.1.1.2
hrSWInstalledLastChange	1.3.6.1.2.1.25.6.1
hrSWInstalledLastUpdateTime	1.3.6.1.2.1.25.6.2
hrSWInstalledIndex	1.3.6.1.2.1.25.6.3.1.1
hrSWInstalledName	1.3.6.1.2.1.25.6.3.1.2
hrSWInstalledID	1.3.6.1.2.1.25.6.3.1.3
hrSWInstalledType	1.3.6.1.2.1.25.6.3.1.4
hrSWInstalledDate	1.3.6.1.2.1.25.6.3.1.5

Table C-7 MTA-MIB

Object	OID
mtaStoredMessages	1.3.6.1.2.1.28.1.1.2
mtaStoredVolume	1.3.6.1.2.1.28.1.1.5
mtaGroupStoredMessages	1.3.6.1.2.1.28.2.1.4
mtaGroupStoredVolume	1.3.6.1.2.1.28.2.1.7
mtaGroupHierarchy	1.3.6.1.2.1.28.2.1.31

Table C-8 IF-MIB

Object	OID
ifName	1.3.6.1.2.1.31.1.1.1.1
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6

Table C-8 IF-MIB (continued)

Object	OID
ifHCInUcastPkts	1.3.6.1.2.1.31.1.1.1.7
ifHCInMulticastPkts	1.3.6.1.2.1.31.1.1.1.8
ifHCInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.9
ifHCOutOctets	1.3.6.1.2.1.31.1.1.1.10
ifHCOutUcastPkts	1.3.6.1.2.1.31.1.1.1.11
ifHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.1.16
ifConnectorPresent	1.3.6.1.2.1.31.1.1.1.17
ifAlias	1.3.6.1.2.1.31.1.1.1.18
ifCounterDiscontinuityTime	1.3.6.1.2.1.31.1.1.1.19
ifTableLastChange	1.3.6.1.2.1.31.1.5

Table C-9 DISMAN-EVENT-MIB

Object	OID
mteResourceSampleMinimum	1.3.6.1.2.1.88.1.1.1
mteResourceSampleInstanceMaximum	1.3.6.1.2.1.88.1.1.2
mteResourceSampleInstances	1.3.6.1.2.1.88.1.1.3
mteResourceSampleInstancesHigh	1.3.6.1.2.1.88.1.1.4
mteResourceSampleInstanceLacks	1.3.6.1.2.1.88.1.1.5
mteTriggerFailures	1.3.6.1.2.1.88.1.2.1
mteTriggerComment	1.3.6.1.2.1.88.1.2.2.1.3
mteTriggerTest	1.3.6.1.2.1.88.1.2.2.1.4
mteTriggerSampleType	1.3.6.1.2.1.88.1.2.2.1.5
mteTriggerValueID	1.3.6.1.2.1.88.1.2.2.1.6
mteTriggerValueIDWildcard	1.3.6.1.2.1.88.1.2.2.1.7
mteTriggerTargetTag	1.3.6.1.2.1.88.1.2.2.1.8
mteTriggerContextName	1.3.6.1.2.1.88.1.2.2.1.9
mteTriggerContextNameWildcard	1.3.6.1.2.1.88.1.2.2.1.10
mteTriggerFrequency	1.3.6.1.2.1.88.1.2.2.1.11
mteTriggerObjectsOwner	1.3.6.1.2.1.88.1.2.2.1.12
mteTriggerObjects	1.3.6.1.2.1.88.1.2.2.1.13
mteTriggerEnabled	1.3.6.1.2.1.88.1.2.2.1.14
mteTriggerEntryStatus	1.3.6.1.2.1.88.1.2.2.1.15
mteTriggerThresholdStartup	1.3.6.1.2.1.88.1.2.6.1.1

Table C-9 DISMAN-EVENT-MIB

Object	OID
mteObjectsID	1.3.6.1.2.1.88.1.3.1.1.3
mteObjectsIDWildcard	1.3.6.1.2.1.88.1.3.1.1.4
mteObjectsEntryStatus	1.3.6.1.2.1.88.1.3.1.1.5
mteEventComment	1.3.6.1.2.1.88.1.4.2.1.2
mteEventActions	1.3.6.1.2.1.88.1.4.2.1.3
mteEventEnabled	1.3.6.1.2.1.88.1.4.2.1.4
mteEventEntryStatus	1.3.6.1.2.1.88.1.4.2.1.5
mteEventNotification	1.3.6.1.2.1.88.1.4.3.1.1
mteEventNotificationObjectsOwner	1.3.6.1.2.1.88.1.4.3.1.2
mteEventNotificationObjects	1.3.6.1.2.1.88.1.4.3.1.3

Table C-10 NOTIFICATION-LOG-MIB

Object	OID
nlmConfigGlobalEntryLimit	1.3.6.1.2.1.92.1.1.1
nlmConfigGlobalAgeOut	1.3.6.1.2.1.92.1.1.2
nlmStatsGlobalNotificationsLogged	1.3.6.1.2.1.92.1.2.1
nlmStatsGlobalNotificationsBumped	1.3.6.1.2.1.92.1.2.2

Table C-11 UCD-SNMP-MIB

Object	OID
prIndex	1.3.6.1.4.1.2021.2.1.1
prNames	1.3.6.1.4.1.2021.2.1.2
prMin	1.3.6.1.4.1.2021.2.1.3
prMax	1.3.6.1.4.1.2021.2.1.4
prCount	1.3.6.1.4.1.2021.2.1.5
prErrorFlag	1.3.6.1.4.1.2021.2.1.100
prErrMessage	1.3.6.1.4.1.2021.2.1.101
prErrFix	1.3.6.1.4.1.2021.2.1.102
prErrFixCmd	1.3.6.1.4.1.2021.2.1.103
memIndex	1.3.6.1.4.1.2021.4.1
memErrorName	1.3.6.1.4.1.2021.4.2
memTotalSwap	1.3.6.1.4.1.2021.4.3
memAvailSwap	1.3.6.1.4.1.2021.4.4
memTotalReal	1.3.6.1.4.1.2021.4.5
memAvailReal	1.3.6.1.4.1.2021.4.6
memTotalFree	1.3.6.1.4.1.2021.4.11

Table C-11 UCD-SNMP-MIB (continued)

Object	OID
memMinimumSwap	1.3.6.1.4.1.2021.4.12
memShared	1.3.6.1.4.1.2021.4.13
memBuffer	1.3.6.1.4.1.2021.4.14
memCached	1.3.6.1.4.1.2021.4.15
memSwapError	1.3.6.1.4.1.2021.4.100
memSwapErrorMsg	1.3.6.1.4.1.2021.4.101
dskIndex	1.3.6.1.4.1.2021.9.1.1
dskPath	1.3.6.1.4.1.2021.9.1.2
dskDevice	1.3.6.1.4.1.2021.9.1.3
dskMinimum	1.3.6.1.4.1.2021.9.1.4
dskMinPercent	1.3.6.1.4.1.2021.9.1.5
dskTotal	1.3.6.1.4.1.2021.9.1.6
dskAvail	1.3.6.1.4.1.2021.9.1.7
dskUsed	1.3.6.1.4.1.2021.9.1.8
dskPercent	1.3.6.1.4.1.2021.9.1.9
dskPercentNode	1.3.6.1.4.1.2021.9.1.10
dskErrorFlag	1.3.6.1.4.1.2021.9.1.100
dskErrorMsg	1.3.6.1.4.1.2021.9.1.101
laIndex	1.3.6.1.4.1.2021.10.1.1
laNames	1.3.6.1.4.1.2021.10.1.2
laLoad	1.3.6.1.4.1.2021.10.1.3
laConfig	1.3.6.1.4.1.2021.10.1.4
laLoadInt	1.3.6.1.4.1.2021.10.1.5
laLoadFloat	1.3.6.1.4.1.2021.10.1.6
laErrorFlag	1.3.6.1.4.1.2021.10.1.100
laErrMessage	1.3.6.1.4.1.2021.10.1.101
ssIndex	1.3.6.1.4.1.2021.11.1
ssErrorName	1.3.6.1.4.1.2021.11.2
ssSwapIn	1.3.6.1.4.1.2021.11.3
ssSwapOut	1.3.6.1.4.1.2021.11.4
ssIOSent	1.3.6.1.4.1.2021.11.5
ssIOReceive	1.3.6.1.4.1.2021.11.6
ssSysInterrupts	1.3.6.1.4.1.2021.11.7
ssSysContext	1.3.6.1.4.1.2021.11.8
ssCpuUser	1.3.6.1.4.1.2021.11.9
ssCpuSystem	1.3.6.1.4.1.2021.11.10

Table C-11 UCD-SNMP-MIB (continued)

Object	OID
ssCpuIdle	1.3.6.1.4.1.2021.11.11
ssCpuRawUser	1.3.6.1.4.1.2021.11.50
ssCpuRawNice	1.3.6.1.4.1.2021.11.51
ssCpuRawSystem	1.3.6.1.4.1.2021.11.52
ssCpuRawIdle	1.3.6.1.4.1.2021.11.53
ssCpuRawWait	1.3.6.1.4.1.2021.11.54
ssCpuRawKernel	1.3.6.1.4.1.2021.11.55
ssCpuRawInterrupt	1.3.6.1.4.1.2021.11.56
ssIORawSent	1.3.6.1.4.1.2021.11.57
ssIORawReceived	1.3.6.1.4.1.2021.11.58
ssRawInterrupts	1.3.6.1.4.1.2021.11.59
ssRawContexts	1.3.6.1.4.1.2021.11.60
ssCpuRawSoftIRQ	1.3.6.1.4.1.2021.11.61
ssRawSwapIn	1.3.6.1.4.1.2021.11.62
ssRawSwapOut	1.3.6.1.4.1.2021.11.63

Table C-12 UCD-DLMOD-MIB

Object	OID
dlmodNextIndex	1.3.6.1.4.1.2021.13.14.1
dlmodName	1.3.6.1.4.1.2021.13.14.2.1.2
dlmodPath	1.3.6.1.4.1.2021.13.14.2.1.3
dlmodError	1.3.6.1.4.1.2021.13.14.2.1.4
dlmodStatus	1.3.6.1.4.1.2021.13.14.2.1.5
diskIOIndex	1.3.6.1.4.1.2021.13.15.1.1.1
diskIODevice	1.3.6.1.4.1.2021.13.15.1.1.2
diskIONRead	1.3.6.1.4.1.2021.13.15.1.1.3
diskIONWritten	1.3.6.1.4.1.2021.13.15.1.1.4
diskIOReads	1.3.6.1.4.1.2021.13.15.1.1.5
diskIOWrites	1.3.6.1.4.1.2021.13.15.1.1.6
diskIOEntry	1.3.6.1.4.1.2021.13.15.1.1
logMatchMaxEntries	1.3.6.1.4.1.2021.16.1
versionIndex	1.3.6.1.4.1.2021.100.1
versionTag	1.3.6.1.4.1.2021.100.2
versionDate	1.3.6.1.4.1.2021.100.3
versionCDate	1.3.6.1.4.1.2021.100.4
versionIdent	1.3.6.1.4.1.2021.100.5

Table C-12 UCD-DLMOD-MIB

Object	OID
versionConfigureOptions	1.3.6.1.4.1.2021.100.6
versionClearCache	1.3.6.1.4.1.2021.100.10
versionUpdateConfig	1.3.6.1.4.1.2021.100.11
versionRestartAgent	1.3.6.1.4.1.2021.100.12
versionSavePersistentData	1.3.6.1.4.1.2021.100.13
versionDoDebugging	1.3.6.1.4.1.2021.100.20
snmperrIndex	1.3.6.1.4.1.2021.101.1
snmperrNames	1.3.6.1.4.1.2021.101.2
snmperrErrorFlag	1.3.6.1.4.1.2021.101.100
snmperrErrMessage	1.3.6.1.4.1.2021.101.101

Table C-13 NET-SNMP-AGENT-MIB

Object	OID
nsMibRegistry	1.3.6.1.4.1.8072.1.2
nsExtensions	1.3.6.1.4.1.8072.1.3
nsCache	1.3.6.1.4.1.8072.1.5
nsConfiguration	1.3.6.1.4.1.8072.1.7

Table C-14 SNMPv2-SMI

Object	OID
snmpSetSerialNo	1.3.6.1.6.3.1.1.6.1

Table C-15 SNMP-FRAMEWORK-MIB

Object	OID
snmpEngineID	1.3.6.1.6.3.10.2.1.1
snmpEngineBoots	1.3.6.1.6.3.10.2.1.2
snmpEngineTime	1.3.6.1.6.3.10.2.1.3
snmpEngineMaxMessageSize	1.3.6.1.6.3.10.2.1.4

Table C-16 SNMP-MPD-MIB

Object	OID
snmpUnknownSecurityModels	1.3.6.1.6.3.11.2.1.1
snmpInvalidMsgs	1.3.6.1.6.3.11.2.1.2
snmpUnknownPDUHandlers	1.3.6.1.6.3.11.2.1.3

Table C-17 SNMP-TARGET-MIB

Object	OID
snmpTargetSpinLock	1.3.6.1.6.3.12.1.1
snmpUnavailableContexts	1.3.6.1.6.3.12.1.4
snmpUnknownContexts	1.3.6.1.6.3.12.1.5

Table C-18 SNMP-USER-BASED-SM-MIB

Object	OID
usmStatsUnsupportedSecLevels	1.3.6.1.6.3.15.1.1.1
usmStatsNotInTimeWindows	1.3.6.1.6.3.15.1.1.2
usmStatsUnknownUserNames	1.3.6.1.6.3.15.1.1.3
usmStatsUnknownEngineIDs	1.3.6.1.6.3.15.1.1.4
usmStatsWrongDigests	1.3.6.1.6.3.15.1.1.5
usmStatsDecryptionErrors	1.3.6.1.6.3.15.1.1.6
usmUserSpinLock	1.3.6.1.6.3.15.1.2.1

Table C-19 SNMP-VIEW-BASED-ACM-MIB

Object	OID
vacmContextName	1.3.6.1.6.3.16.1.1.1.1
vacmGroupName	1.3.6.1.6.3.16.1.2.1.3
vacmSecurityToGroupStorageType	1.3.6.1.6.3.16.1.2.1.4
vacmSecurityToGroupStatus	1.3.6.1.6.3.16.1.2.1.5
vacmAccessContextMatch	1.3.6.1.6.3.16.1.4.1.4
vacmAccessReadViewName	1.3.6.1.6.3.16.1.4.1.5
vacmAccessWriteViewName	1.3.6.1.6.3.16.1.4.1.6
vacmAccessNotifyViewName	1.3.6.1.6.3.16.1.4.1.7
vacmAccessStorageType	1.3.6.1.6.3.16.1.4.1.8
vacmAccessStatus	1.3.6.1.6.3.16.1.4.1.9
vacmViewSpinLock	1.3.6.1.6.3.16.1.5.1
vacmViewTreeFamilyMask	1.3.6.1.6.3.16.1.5.2.1.3
vacmViewTreeFamilyType	1.3.6.1.6.3.16.1.5.2.1.4
vacmViewTreeFamilyStorageType	1.3.6.1.6.3.16.1.5.2.1.5
vacmViewTreeFamilyStatus	1.3.6.1.6.3.16.1.5.2.1.6



Open Source License Acknowledgments

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

   The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].



INDEX

A

Active Directory 7-16, 7-27
Add Exempt Device 11-12
Add Floating Device 11-16
admin console
  Server 14-58
admin password, changing 14-56
Agent 9-1, 10-27
  checks 9-72
  reports 11-1

B

Backup 14-59
Bandwidth
  limiting usage 8-13
bursting 8-14

C

CAS management pages 1-23
certificate. See SSL certificate.
Certified Devices
  overview 11-10
CSR, generating 14-12

D

Domain Name field 7-5, 7-15, 7-17, 7-19

E

Event Logs 13-4
  Event column 13-7
  Logs Setting 13-9
  Log Viewer 13-4
  messages A-2 to A-5
  Syslog Setting 13-10

F

File Upload 5-13
filter policies
  by subnet 2-27
floating devices 11-16
fragmentation, IP packet 8-6

G

global settings 2-8
guest access 5-17

H

HA-Primary mode 14-4
HA-Standby mode 14-4
Heartbeat Timer 8-18

I

IP fragment packets 8-6
IP Setting tab 14-4

K

Kerberos authentication
settings 7-5
Kick All Users command 11-34

L

LDAP authentication, configuring 7-16
local settings 2-9
Local Users 6-15
log events A-2 to A-5
logging
event logs 13-4
user activity 13-4
Logout Page 5-16

M

Monitoring
overview 13-1
MS Update Scanning Tool 11-41

N

NAS RADIUS properties 7-7, 7-41
Nessus plugins 12-1
Network Scanning 12-1

O

Online Users
overview 11-28

P

passthrough policies
by subnet 2-27
password, admin 14-56
Plugins 12-6
Provider dropdown 7-3

Q

quarantine role, configuring 8-22, 12-6

R

RADIUS authentication 7-6
reboot Server 2-8
Reports
Agent 11-1
network scanner 12-17
roles, user 6-2 to 6-14
default policies 8-2
deleting 6-15
rules
creating 9-80

S

Server
admin console, opening 14-58
Delete (Remove) 2-8
Manage 2-4
reboot 2-8
system stats 13-4, 13-7, 13-9
service perfigo config 2-8
Session Timer 8-17
Shared Secret
RADIUS 7-7
SSL Certificate
Certificate-Related Files 14-24
Export Certificate Request 14-12, 14-14
Generate Temporary Certificate 14-11
Import Signed Certificate 14-14

overview 14-7
Troubleshooting 14-21
SSL certificate
exporting CSR 14-12
standalone mode 14-4
subnet, managing access 2-27
syslog 13-4, 13-10
system stats 13-4, 13-7, 13-9

T

Temporary role 8-20, 9-12
terminate user sessions 11-33
terminating user sessions 11-34
test
authentication 7-38
network scanning 12-16
Timer, certified device clearing 11-14
time server 14-5

U

User Management 5-1, 6-1, 7-1, 11-28
activity logs 13-4
guest access 5-17
Mapping Rules 7-30
terminate sessions 11-33
user management
terminating sessions 11-34

V

Verify Rules 9-81
vulnerabilities 12-13

W

Windows NT authentication 7-15
Windows Script 5.6 11-41